HIRSCHMANN
A BELDEN BRAND

User Manual

Basic Configuration
Industrial ETHERNET (Gigabit) Switch
RS20/RS30/RS40, MS20/MS30, OCTOPUS

Technical Support
HAC.Support@Belden.com

The naming of copyrighted trademarks in this manual, even when not specially indicated, should not be taken to mean that these names may be considered as free in the sense of the trademark and tradename protection law and hence that they may be freely used by anyone.

© 2010Hirschmann Automation and Control GmbH

Manuals and software are protected by copyright. All rights reserved. The copying, reproduction, translation, conversion into any electronic medium or machine scannable form is not permitted, either in whole or in part. An exception is the preparation of a backup copy of the software for your own use. For devices with embedded software, the end-user license agreement on the enclosed CD applies.

The performance features described here are binding only if they have been expressly agreed when the contract was made. This document was produced by Hirschmann Automation and Control GmbH according to the best of the company's knowledge. Hirschmann reserves the right to change the contents of this document without prior notice. Hirschmann can give no guarantee in respect of the correctness or accuracy of the information in this document.

Hirschmann can accept no responsibility for damages, resulting from the use of the network components or the associated operating software. In addition, we refer to the conditions of use specified in the license contract.

You can get the latest version of this manual on the Internet at the Hirschmann product site (www.hirschmann-ac.de).

Printed in Germany
Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Germany
Tel.: +49 1805 141538

Contents

About this Manual 7

Key 9

Introduction 11

1 Access to the user interfaces 13

1.1 System Monitor 14

1.2 Command Line Interface 16

1.3 Web-based Interface 19

2 Entering the IP Parameters 23

2.1 IP Parameter Basics 25
2.1.1 IP address (version 4) 25
2.1.2 Netmask 26
2.1.3 Classless Inter-Domain Routing 29

2.2 Entering IP parameters via CLI 31

2.3 Entering the IP Parameters via HiDiscovery 34

2.4 Loading the system configuration from the ACA 37

2.5 System configuration via BOOTP 39

2.6 System Configuration via DHCP 44

2.7 System Configuration via DHCP Option 82 47

2.8 Web-based IP Configuration 48

2.9 Faulty Device Replacement 50

3 Loading/saving settings 51

3.1 Loading settings 52
3.1.1 Loading from the local non-volatile memory 53
3.1.2 Loading from the AutoConfiguration Adapter 53
3.1.3 Loading from a file 54
3.1.4 Resetting the configuration to the state on delivery 56

3.2 Saving settings 57
3.2.1 Saving locally (and on the ACA) 57

3.2.2 Saving to a file on URL 58

4 Loading Software Updates 61

4.1 Loading the Software manually from the ACA 63
4.1.1 Selecting the software to be loaded 64
4.1.2 Starting the software 65
4.1.3 Performing a cold start 65

4.2 Automatic software update by ACA 66

4.3 Loading the software from the tftp server 68

4.4 Loading the Software via File Selection 70

5 Configuring the Ports 71

6 Protection from Unauthorized Access 75

6.1 Protecting the device 76

6.2 Password for SNMP access 77
6.2.1 Description of password for SNMP access 77
6.2.2 Entering the password for SNMP access 78

6.3 Telnet/Web Access 81
6.3.1 Description of Telnet Access 81
6.3.2 Description of Web Access 81
6.3.3 Enabling/disabling Telnet/Web Access 82

6.4 HiDiscovery Access 83
6.4.1 Description of the HiDiscovery Protocol 83
6.4.2 Enabling/disabling the HiDiscovery Function 83

7 Synchronizing the System Time in the Network 89

7.1 Entering the Time 90

7.2 SNTP 92
7.2.1 Description of SNTP 92
7.2.2 Preparing the SNTP Configuration 93
7.2.3 Configuring SNTP 94

7.3 Precision Time Protocol 98
7.3.1 Description of PTP Functions 98

8 Network Load Control 103

8.1 Direct Packet Distribution 104
8.1.1 Store-and-forward 104
8.1.2 Multi-Address Capability 104

8.1.3 Aging of Learned Addresses 105
8.1.4 Entering Static Addresses 106
8.1.5 Disabling the Direct Packet Distribution 107

8.2 Multicast Application 108
8.2.1 Description of the Multicast Application 108
8.2.2 Example of a Multicast Application 109
8.2.3 Description of IGMP Snooping 110
8.2.4 Setting IGMP Snooping 111
8.2.5 Setting GMRP 117

8.3 Rate Limiter 118
8.3.1 Description of the Rate Limiter 118
8.3.2 Rate Limiter settings 119

8.4 QoS/Priority 121
8.4.1 Description of Prioritization 121
8.4.2 VLAN tagging 122
8.4.3 IP ToS / DiffServ 124
8.4.4 Handling of Received Priority Information 127
8.4.5 Handling of Traffic Classes 127
8.4.6 Setting prioritization 128

8.5 Flow Control 132
8.5.1 Description of Flow Control 132
8.5.2 Setting the Flow Control 134

8.6 VLANs 135
8.6.1 VLAN Description 135
8.6.2 Examples of VLANs 136

9 Operation Diagnosis 153

9.1 Sending Traps 154
9.1.1 List of SNMP Traps 155
9.1.2 SNMP Traps during Boot 156
9.1.3 Configuring Traps 157

9.2 Monitoring the Device Status 159
9.2.1 Configuring the Device Status 160
9.2.2 Displaying the Device Status 161

9.3 Out-of-band Signaling 162
9.3.1 Controlling the Signal Contact 163
9.3.2 Monitoring the Device Status via the Signal Contact 163
9.3.3 Monitoring the Device Functions via the Signal Contact 164

9.4 Port Status Indication 166

9.5 Event Counter at Port Level 167

9.5.1 Detecting Non-matching Duplex Modes 168
9.6 Displaying the SFP Status 172
9.7 Topology Discovery 173
9.7.1 Description of Topology Discovery 173
9.7.2 Displaying the Topology Discovery Results 175
9.8 Detecting IP Address Conflicts 178
9.8.1 Description of IP Address Conflicts 178
9.8.2 Configuring ACD 179
9.8.3 Displaying ACD 180
9.9 Detecting Loops 181
9.10 Reports 182
9.11 Monitoring Data Traffic at Ports (Port Mirroring) 184
9.12 Syslog 187
9.13 Event Log 188

A Setting up the Configuration Environment 189

B General Information 205

C Index 213

D Further Support 217

About this Manual

The “Basic Configuration” user manual contains the information you need to start operating the device. It takes you step by step from the first startup operation through to the basic settings for operation in your environment.

The following thematic sequence has proven itself in practice:

- Set up device access for operation by entering the IP parameters
- Check the status of the software and update it if necessary
- If a configuration already exists, load/store it
- Configure the ports
- Set up protection from unauthorized access
- Optimize the data transmission with network load control
- Synchronize system time in the network
- Function diagnosis
- Store the newly created configuration to nonvolatile memory

The “Installation” user manual contains a device description, safety instructions, a description of the display, and the other information that you need to install the device.

The “Redundancy Configuration” user manual contains the information you need to select a suitable redundancy procedure and configure that procedure.

The “Industry Protocols” user manual describes how the device is connected by means of a communication protocol commonly used in the industry, such as EtherNet/IP and PROFINET IO.

The "Web-based Interface" reference manual contains detailed information on using the Web interface to operate the individual functions of the device.

The "Command Line Interface" reference manual contains detailed information on using the Command Line Interface to operate the individual functions of the device.

The Network Management Software HiVision/Industrial HiVision provides you with additional options for smooth configuration and monitoring:

- Configuration of multiple devices simultaneously.
- Graphical interface with network layouts.
- Auto-topology discovery.
- Event log.
- Event handling.
- Client / Server structure.
- Browser interface
- ActiveX control for SCADA integration
- SNMP/OPC gateway

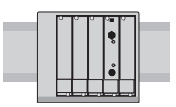
Key

The designations used in this manual have the following meanings:

▶	List
☐	Work step
■	Subheading
Link	Indicates a cross-reference with a stored link
Note:	A note emphasizes an important fact or draws your attention to a dependency.
`Courier`	ASCII representation in user interface
	Execution in the Web-based Interface user interface
	Execution in the Command Line Interface user interface

Symbols used:

	WLAN access point
	Router with firewall
	Switch with firewall
	Router
	Switch

	Bridge
	Hub
	A random computer
	Configuration Computer
	Server
	PLC - Programmable logic controller
	I/O - Robot

Introduction

The device has been developed for practical application in a harsh industrial environment. Accordingly, the installation process has been kept simple. Thanks to the selected default settings, you only have to enter a few settings before starting to operate the device.

Note: The changes you make in the dialogs are copied into the volatile memory of the device when you click on "Set".
To save the changes into the permanent memory of the device select the non-volatile memory location in the `Basic Settings:Load/Save` dialog and click "Save".

1 Access to the user interfaces

The device has 3 user interfaces, which you can access via different interfaces:

- System monitor via the V.24 interface (out-of-band)
- Command Line Interface (CLI) via the V.24 connection (out-of-band) and Telnet (in-band)
- Web-based interface via Ethernet (in-band).

1.1 System Monitor

The system monitor enables you to

- select the software to be loaded
- perform a software update
- start the selected software
- shut down the system monitor
- delete the configuration saved and
- display the boot code information.

Opening the system monitor

☐ Use the terminal cable (see accessories) to connect
  – the V.24 socket (RJ11) to
  – a terminal or a COM port of a PC with terminal emulation based on VT100
  (for the physical connection, see the "Installation" user manual).

Speed	9,600 Baud
Data	8 bit
Parity	none
Stopbit	1 bit
Handshake	off

Table 1: Data transfer parameters

☐ Start the terminal program on the PC and set up a connection with the device.

When you boot the device, the message
"Press <1> to enter System Monitor 1"
appears on the terminal.

```
< Device Name  (Boot) Release: 1.00 Build: 2005-09-17 15:36 >

Press <1> to enter System Monitor 1 ...
 1
```

Figure 1: Screen display during the boot process

☐ Press the <1> key within one second to start system monitor 1.

```
   System Monitor

   (Selected OS: L3P-01.0.00-K16 (2005-10-31 19:32))

   1  Select Boot Operating System
   2  Update Operating System
   3  Start Selected Operating System
   4  End (reset and reboot)
   5  Erase main configuration file




sysMon1>
```

Figure 2: System monitor 1 screen display

☐ Select a menu item by entering the number.
☐ To leave a submenu and return to the main menu of system monitor 1, press the <ESC> key.

1.2 Command Line Interface

The Command Line Interface enables you to use the functions of the device via a local or remote connection.
The Command Line Interface provides IT specialists with a familiar environment for configuring IT devices.
The script compatibility of the Command Line Interface enables you, among other things, to feed multiple devices with the same configuration data, to create and apply partial configurations or to compare 2 configuration by comparing the script files.

You will find a detailed description of the Command Line Interface in the "Command Line Interface" reference manual.

You can access the Command Line Interface via

- the V.24 port (out-of-band)
- Telnet (in-band)

Note: To facilitate making entries, CLI gives you the option of abbreviating keywords. Type in the beginning of a keyword. When you press the tab key, CLI completes the keyword.

Opening the Command Line Interface

☐ Connect the device to a terminal or to the COM port of a PC using terminal emulation based on VT100 and press any key (see on page 14 “Opening the system monitor“) or
call up the Command Line Interface via Telnet.
A window for entering the user name appears on the screen.
Up to five users can access the Command Line Interface.

```
        Copyright (c) 2004-2009 Hirschmann Automation and Control GmbH

                             All rights reserved

                          PowerMICE Release L3P-05.1.00

                          (Build date 2009-10-11 12:13)



                        System Name:  PowerMICE
                        Mgmt-IP    :  10.0.1.105
                        1.Router-IP:  0.0.0.0
                        Base-MAC   :  00:80:63:51:74:00
                        System Time:  2009-10-11 13:14:15


User:
```

Figure 3: Logging in to the Command Line Interface program

- ☐ Enter a user name. The default setting for the user name is **admin** . Press the Enter key.
- ☐ Enter the password. The default setting for the password is **private** . Press the Enter key.
  You can change the user name and the password later in the Command Line Interface.
  Please note that these entries are case-sensitive.

The start screen appears.

```
NOTE: Enter '?' for Command Help. Command help displays all options
      that are valid for the 'normal' and 'no' command forms.  For
      the syntax of a particular command form, please consult the
      documentation.


(Hirschmann Product) >
```

Figure 4: CLI screen after login

1.3 Web-based Interface

The user-friendly Web-based interface gives you the option of operating the device from any location in the network via a standard browser such as Mozilla Firefox or Microsoft Internet Explorer.
As a universal access tool, the Web browser uses an applet which communicates with the device via the Simple Network Management Protocol (SNMP).
The Web-based interface allows you to graphically configure the device.

Opening the Web-based Interface

To open the Web-based interface, you need a Web browser (a program that can read hypertext), for example Mozilla Firefox version 1 or later, or Microsoft Internet Explorer version 6 or later.

Note: The Web-based interface uses Java software 6 (“Java™ Runtime Environment Version 1.6.x”).

Install the software from the enclosed CD-ROM. To do this, you go to “Additional Software”, select `Java Runtime Environment` and click on “Installation”.

Device Software
Device Info
AddOn Software
AddOn Info
Imprint
Exit
Java Runtime Environment 5
The Web-based interface uses the " Java™ Runtime Environment" plug-in. The Web-based interface of this device has been tested with the version of the plug-in on this CD-ROM.
JAVA™ 2 PLATFORM STANDARD EDITION
haneWIN DHCP-Server 2.0.29
Adobe Acrobat Reader
Java Runtime Environment 5
Instal
Website

Figure 5: Installing Java

- ☐ Start your Web browser.
- ☐ Check that you have activated JavaScript and Java in your browser settings.
- ☐ Establish the connection by entering the IP address of the device which you want to administer via the Web-based management in the address field of the Web browser. Enter the address in the following form:
  `http://xxx.xxx.xxx.xxx`

  The login window appears on the screen.

Figure 6: Login window

- ☐ Select the desired language.
- ☐ In the drop-down menu, you select
  – user, to have read access, or
  – admin, to have read and write access

  to the device.
- ☐ The password "public", with which you have read access, appears in the password field. If you wish to have write access to the device, then highlight the contents of the password field and overwrite it with the password "private" (default setting).
- ☐ Click on OK.

The website of the device appears on the screen.

Note: The changes you make in the dialogs are copied to the device when you click "Set". Click "Reload" to update the display.

Note: You can block your access to the device by entering an incorrect configuration.
Activating the function "Cancel configuration change" in the "Load/Save" dialog enables you to return automatically to the last configuration after a set time period has elapsed. This gives you back your access to the device.

2 Entering the IP Parameters

The IP parameters must be entered when the device is installed for the first time.

The device provides 7 options for entering the IP parameters during the first installation:

- Entry using the Command Line Interface (CLI).
  You choose this “out of band” method if
  - you preconfigure your device outside its operating environment
  - you do not have network access (“in-band”) to the device

  (see page 31 “Entering IP parameters via CLI“).
- Entry using the HiDiscovery protocol.
  You choose this “in-band” method if the device is already installed in the network or if you have another Ethernet connection between your PC and the device
  (see page 34 “Entering the IP Parameters via HiDiscovery“).
- Configuration using the AutoConfiguration Adapter (ACA).
  You choose this method if you are replacing a device with a device of the same type and have already saved the configuration on an ACA(see page 37 “Loading the system configuration from the ACA“).
- Using BOOTP.
  You choose this “in-band” method if you want to configure the installed device using BOOTP. You need a BOOTP server for this. The BOOTP server assigns the configuration data to the device using its MAC address (see page 39 “System configuration via BOOTP“). Because the device is delivered with “DHCP mode” as the entry for the configuration data reference, you have to reset this to the BOOTP mode for this method.
- Configuration via DHCP.
  You choose this “in-band” method if you want to configure the installed device using DHCP. You need a DHCP server for this. The DHCP server assigns the configuration data to the device using its MAC address or its system name (see page 44 “System Configuration via DHCP“).

- Using DHCP Option 82.
  You choose this “in-band” method if you want to configure the installed device using DHCP Option 82. You need a DHCP server with Option 82 for this. The DHCP server assigns the configuration data to the device using its physical connection (see page 47 “System Configuration via DHCP Option 82“).
- Configuration via the Web-based interface.
  If the device already has an IP address and can be reached via the network, then the Web-based interface provides you with another option for configuring the IP parameters.

2.1 IP Parameter Basics

2.1.1 IP address (version 4)

The IP addresses consist of 4 bytes. These 4 bytes are written in decimal notation, separated by a decimal point.

Since 1992, five classes of IP address have been defined in the RFC 1340.

Class	Network address	Host address	Address range
A	1 byte	3 bytes	1.0.0.0 to 126.255.255.255
B	2 bytes	2 bytes	128.0.0.0 to 191.255.255.255
C	3 bytes	1 byte	192.0.0.0 to 223.255.255.255
D			224.0.0.0 to 239.255.255.255
E			240.0.0.0 to 255.255.255.255

Table 2: IP address classes

The network address is the fixed part of the IP address. The worldwide leading regulatory board for assigning network addresses is the IANA (Internet Assigned Numbers Authority). If you require an IP address block, contact your Internet service provider. Internet service providers should contact their local higher-level organization:

- APNIC (Asia Pacific Network Information Center) - Asia/Pacific Region
- ARIN (American Registry for Internet Numbers) - Americas and Sub-Sahara Africa
- LACNIC (Regional Latin-American and Caribbean IP Address Registry) – Latin America and some Caribbean Islands
- RIPE NCC (Réseaux IP Européens) - Europe and Surrounding Regions

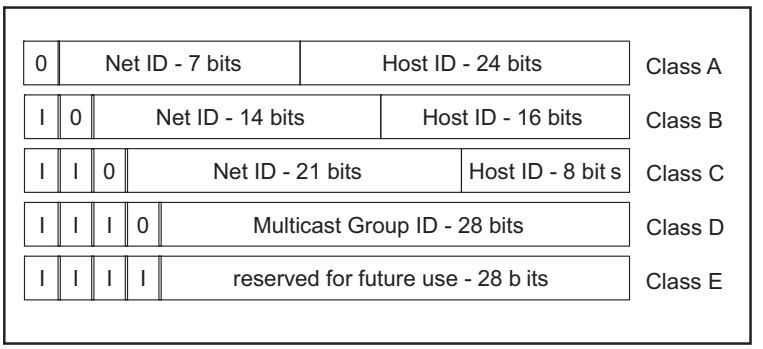


Figure 7: Bit representation of the IP address

An IP address belongs to class A if its first bit is a zero, i.e. the first decimal number is less than 128. The IP address belongs to class B if the first bit is a one and the second bit is a zero, i.e. the first decimal number is between 128 and 191. The IP address belongs to class C if the first two bits are a one, i.e. the first decimal number is higher than 191.

Assigning the host address (host id) is the responsibility of the network operator. He alone is responsible for the uniqueness of the IP addresses he assigns.

2.1.2 Netmask

Routers and gateways subdivide large networks into subnetworks. The netmask assigns the IP addresses of the individual devices to a particular subnetwork.

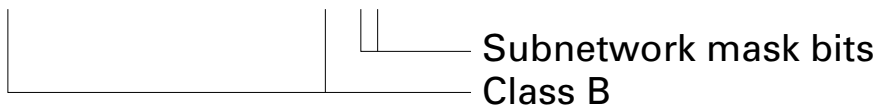
The division into subnetworks with the aid of the netmask is performed in much the same way as the division of the network addresses (net id) into classes A to C.

The bits of the host address (host id) that represent the mask are set to one. The remaining bits of the host address in the netmask are set to zero (see the following examples).

Example of a netmask:

Decimal notation
255.255.192.0

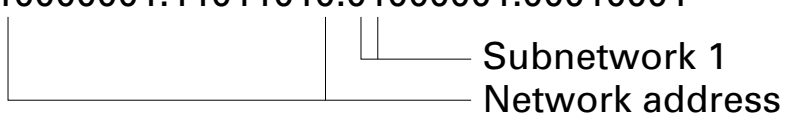
Binary notation
11111111.11111111.11000000.00000000



Example of IP addresses with subnetwork assignment when the above subnet mask is applied:

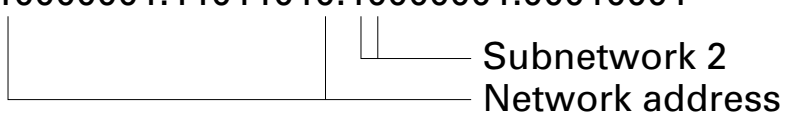
Decimal notation
129.218.65.17

binary notation
10000001.11011010.01000001.00010001



Decimal notation
129.218.129.17

binary notation
10000001.11011010.10000001.00010001



Example of how the network mask is used

In a large network it is possible that gateways and routers separate the management agent from its management station. How does addressing work in such a case?

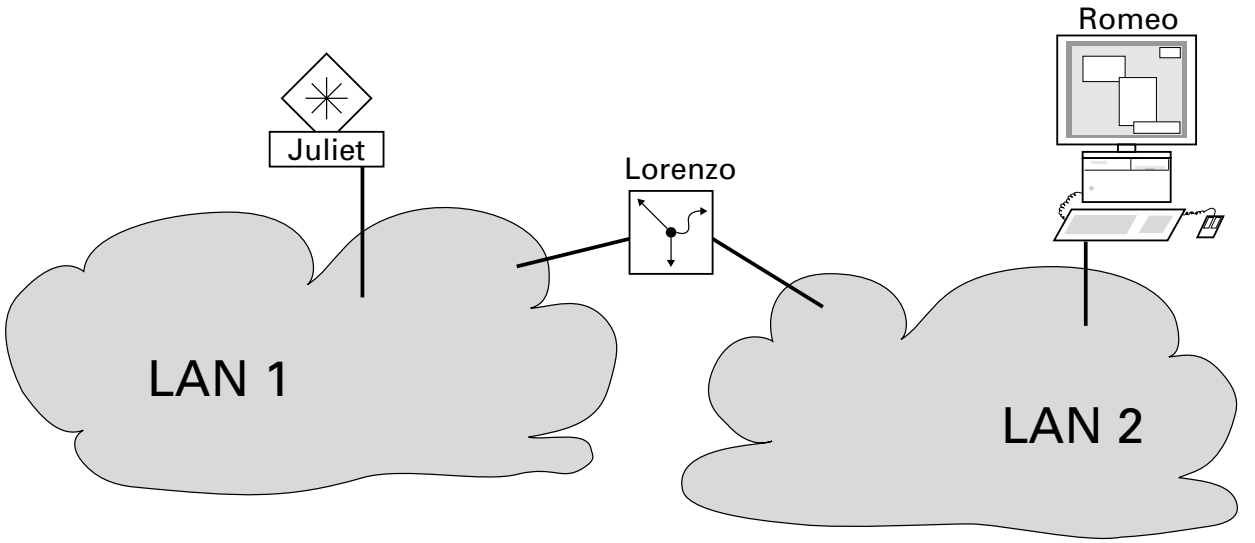


Figure 8: Management agent that is separated from its management station by a router

The management station "Romeo" wants to send data to the management agent "Juliet". Romeo knows Juliet's IP address and also knows that the router "Lorenzo" knows the way to Juliet.

Romeo therefore puts his message in an envelope and writes Juliet's IP address as the destination address. For the source address he writes his own IP address on the envelope.

Romeo then places this envelope in a second one with Lorenzo's MAC address as the destination and his own MAC address as the source. This process is comparable to going from layer 3 to layer 2 of the ISO/OSI base reference model.

Finally, Romeo puts the entire data packet into the mailbox. This is comparable to going from layer 2 to layer 1, i.e. to sending the data packet over the Ethernet.

Lorenzo receives the letter and removes the outer envelope. From the inner envelope he recognizes that the letter is meant for Juliet. He places the inner envelope in a new outer envelope and searches his address list (the ARP table) for Juliet's MAC address. He writes her MAC address on the outer envelope as the destination address and his own MAC address as the source address. He then places the entire data packet in the mail box.

Juliet receives the letter and removes the outer envelope. She finds the inner envelope with Romeo's IP address. Opening the inner envelope and reading its contents corresponds to transferring the message to the higher protocol layers of the SO/OSI layer model.

Juliet would now like to send a reply to Romeo. She places her reply in an envelope with Romeo's IP address as destination and her own IP address as source. But where is she to send the answer? For she did not receive Romeo's MAC address. It was lost when Lorenzo replaced the outer envelope.

In the MIB, Juliet finds Lorenzo listed under the variable hmNetGatewayIPAddr as a means of communicating with Romeo. She therefore puts the envelope with the IP addresses in a further envelope with Lorenzo's MAC destination address.

The letter now travels back to Romeo via Lorenzo, the same way the first letter traveled from Romeo to Juliet.

2.1.3 Classless Inter-Domain Routing

Class C with a maximum of 254 addresses was too small, and class B with a maximum of 65534 addresses was too large for most users, as they would never require so many addresses. This resulted in ineffective usage of the class B addresses available.
Class D contains reserved multicast addresses. Class E is reserved for experimental purposes. A gateway not participating in these experiments ignores datagrams with these destination addresses.

Since 1993, RFC 1519 has been using Classless Inter Domain Routing (CIDR) to provide a solution to get around these problems. CIDR overcomes these class boundaries and supports classless address ranges.

With CIDR, you enter the number of bits that designate the IP address range. You represent the IP address range in binary form and count the mask bits that designate the netmask. The netmask indicates the number of bits that are identical to the network part for all IP addresses in a given address range. Example:

IP address, decimal	Network mask, decimal	IP address, hexadecimal
149.218.112.1	255.255.255.128	10010101 11011010 01110000 00000001
149.218.112.127		10010101 11011010 01110000 01111111

25 mask bits

CIDR notation: 149.218.112.0/25

Mask bits

The combination of a number of class C address ranges is known as “supernetting”. This enables you to subdivide class B address ranges to a very fine degree.

2.2 Entering IP parameters via CLI

If you do not configure the system via BOOTP/DHCP, DHCP Option 82, the HiDiscovery protocol or the AutoConfiguration AdapterACA, then you perform the configuration via the V.24 interface using the CLI.

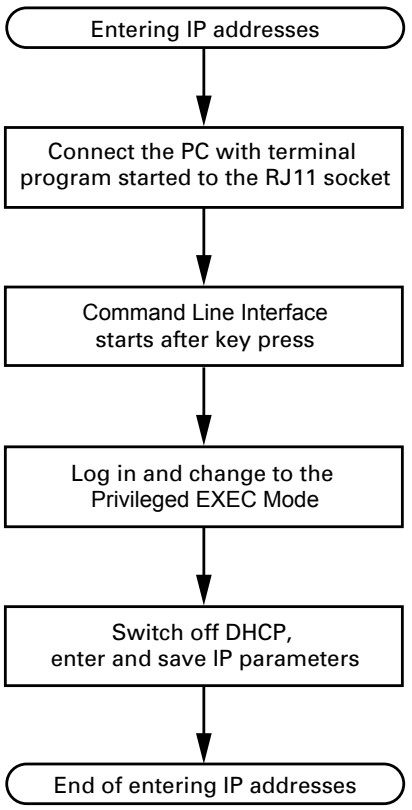

Entering IP addresses
Connect the PC with terminal program started to the RJ11 socket
Command Line Interface starts after key press
Log in and change to the Privileged EXEC Mode
Switch off DHCP, enter and save IP parameters
End of entering IP addresses

Figure 9: Flow chart for entering IP addresses

Note: If there is no terminal or PC with terminal emulation available in the vicinity of the installation location, you can configure the device at your own workstation, then take it to its final installation location.

☐ Set up a connection to the device (see on page 16 “Opening the Command Line Interface“).

The start screen appears.

```
NOTE: Enter '?' for Command Help. Command help displays all options
      that are valid for the 'normal' and 'no' command forms.  For
      the syntax of a particular command form, please consult the
      documentation.


(Hirschmann PowerMICE) >
```

☐ Deactivate DHCP.

☐ Enter the IP parameters.

- Local IP address
  On delivery, the device has the local IP address 0.0.0.0.
- Netmask
  If your network has been divided up into subnetworks, and if these are identified with a netmask, then the netmask is to be entered here.
  The default setting of the netmask is 0.0.0.0.
- IP address of the gateway
  This entry is only required if the device and the management station or tftp server are located in different subnetworks (see page 28 “Example of how the network mask is used“).
  Enter the IP address of the gateway between the subnetwork with the device and the path to the management station.
  The default setting of the IP address is 0.0.0.0.

☐ Save the configuration entered using
`copy system:running-config nvram:startup-config`.

`enable`	Switch to the Privileged EXEC mode.
`network protocol none`	Deactivate DHCP.
`network parms 10.0.1.23 255.255.255.0`	Assign the device the IP address 10.0.1.23 and the netmask 255.255.255.0. You have the option of also assigning a gateway address.
`copy system:running-config nvram:startup-config`	Save the current configuration to the non-volatile memory.

After entering the IP parameters, you can easily configure the device via the Web-based interface (see the “Web-based Interface” reference manual).

2.3 Entering the IP Parameters via HiDiscovery

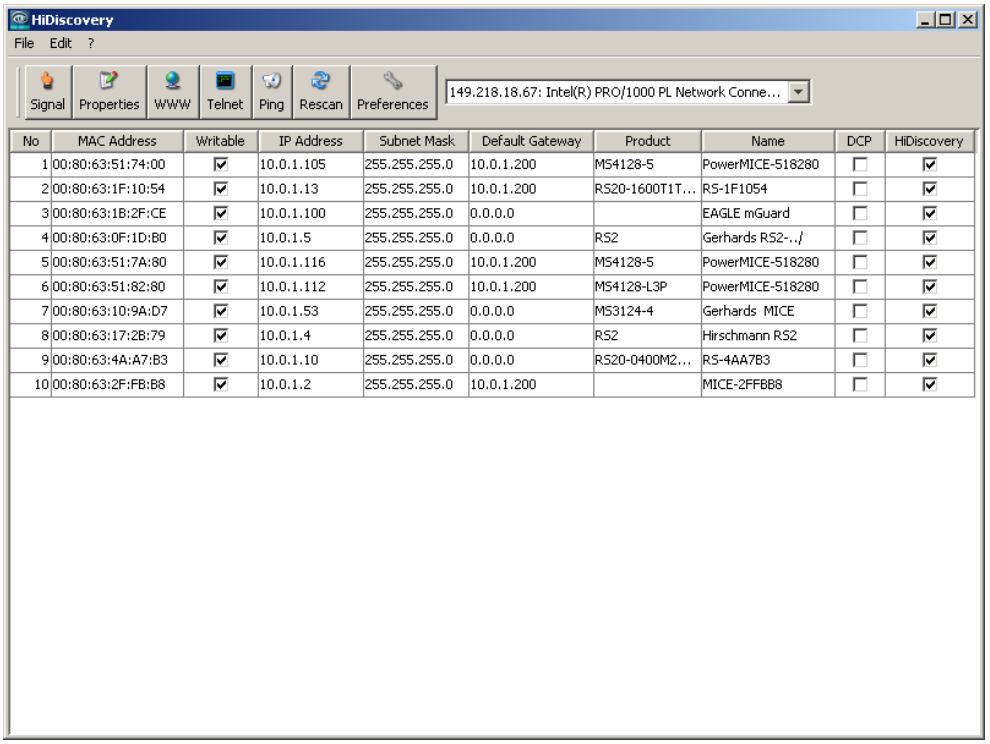
The HiDiscovery protocol enables you to assign IP parameters to the device via the Ethernet.
You can easily configure other parameters via the Web-based interface (see the "Web-based Interface" reference manual).

Install the HiDiscovery software on your PC. The software is on the CD supplied with the device.

☐ To install it, you start the installation program on the CD.

Note: The installation of HiDiscovery includes the installation of the software package WinPcap Version 3.1.
If an earlier version of WinPcap is on the PC, the follow the suggestion in the set-up to uninstall it.
A newer version remains intact during the installationHiDiscovery. However, this cannot be guaranteed for all future versions of WinPcap. In the event that the installation of HiDiscovery has overwritten a newer version of WinPcap, you uninstall WinPcap 3.1 and then re-install the new version.

☐ Start the HiDiscovery program.



No	MAC Address	Writable	IP Address	Subnet Mask	Default Gateway	Product	Name	DCP	HiDiscovery
1	00:80:63:51:74:00	☑	10.0.1.105	255.255.255.0	10.0.1.200	MS4128-5	PowerMICE-518280	☐	☑
2	00:80:63:1F:10:54	☑	10.0.1.13	255.255.255.0	10.0.1.200	RS20-1600T1T...	RS-1F1054	☐	☑
3	00:80:63:1B:2F:CE	☑	10.0.1.100	255.255.255.0	0.0.0.0		EAGLE mGuard	☐	☑
4	00:80:63:0F:1D:B0	☑	10.0.1.5	255.255.255.0	0.0.0.0	RS2	Gerhards RS2-../	☐	☑
5	00:80:63:51:7A:80	☑	10.0.1.116	255.255.255.0	10.0.1.200	MS4128-5	PowerMICE-518280	☐	☑
6	00:80:63:51:82:80	☑	10.0.1.112	255.255.255.0	10.0.1.200	MS4128-L3P	PowerMICE-518280	☐	☑
7	00:80:63:10:9A:D7	☑	10.0.1.53	255.255.255.0	0.0.0.0	MS3124-4	Gerhards MICE	☐	☑
8	00:80:63:17:2B:79	☑	10.0.1.4	255.255.255.0	0.0.0.0	RS2	Hirschmann RS2	☐	☑
9	00:80:63:4A:A7:B3	☑	10.0.1.10	255.255.255.0	0.0.0.0	RS20-0400M2...	RS-4AA7B3	☐	☑
10	00:80:63:2F:FB:B8	☑	10.0.1.2	255.255.255.0	10.0.1.200		MICE-2FFBB8	☐	☑

Figure 10: HiDiscovery

When HiDiscovery is started, it automatically searches the network for those devices which support the HiDiscovery protocol.
HiDiscovery uses the first PC network card found. If your computer has several network cards, you can select these in HiDiscovery on the toolbar.

HiDiscovery displays a line for every device which reacts to the HiDiscovery protocol.

HiDiscovery enables you to identify the devices displayed.

☐ Select a device line.

☐ Click on the signal symbol in the tool bar to set the LEDs for the selected device flashing. To switch off the flashing, click on the symbol again.

☐ By double-clicking a line, you open a window in which you can enter the device name and the IP parameters.

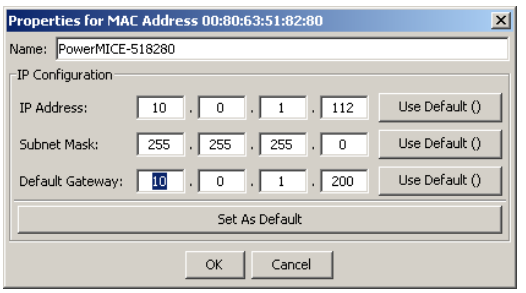


Figure 11: HiDiscovery - assigning IP parameters

Note: When the IP address is entered, the device copies the local configuration settings (see on page 51 “Loading/saving settings“).

Note: For security reasons, switch off the HiDiscovery function for the device in the Web-based interface, after you have assigned the IP parameters to the device (see on page 48 “Web-based IP Configuration“).

Note: Save the settings so that you will still have the entries after a restart (see on page 51 “Loading/saving settings“).

2.4 Loading the system configuration from the ACA

The AutoConfiguration Adapter (ACA) is a device for

- storing the configuration data of a device and
- storing the device software.

In the case of a device becoming inoperative, the ACA makes it possible to easily transfer the configuration data by means of a substitute device of the same type.

When you start the device, it checks for an ACA. If it finds an ACA with a valid password and valid software, the device loads the configuration data from the ACA.

The password is valid if

- the password in the device matches the password in the ACA or
- the preset password is entered in the device.

To save the configuration data on the ACA(see on page 57 “Saving locally (and on the ACA)“).

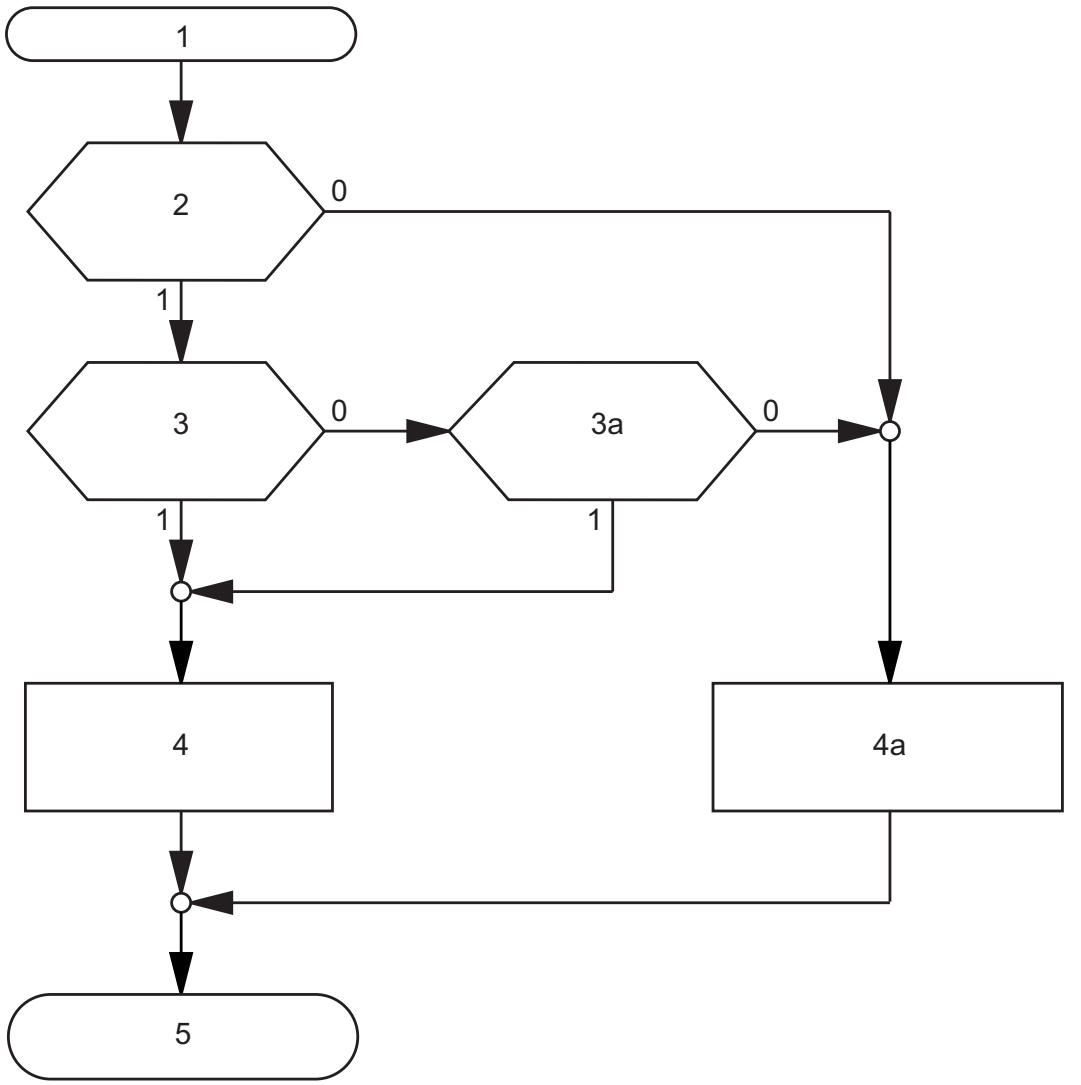


Figure 12: Flow chart of loading configuration dats from the ACA

1 – Device start-up
2 – ACA plugged-in?
3 – Password in device and ACA identical?
3a – Default password in device?
4 – Load configuration from ACA,
ACA LEDs flashing synchronously
4a –Load configuration from local memory,
ACA LEDs flashing alternately
5 – Configuration data loaded

2.5 System configuration via BOOTP

When it is started up via BOOTP (bootstrap protocol), a device receives its configuration data in accordance with the “BOOTP process” flow chart (see fig. 13).

Note: In its delivery state, the device gets its configuration data from the DHCP server.

☐ Activate BOOTP to receive the configuration data (see on page 48 “Web-based IP Configuration“), or see the CLI:

`enable`	Switch to the Privileged EXEC mode.
`network protocol bootp`	Activate BOOTP.
`copy system:running-config nvram:startup-config`	Activate BOOTP.
`y`	Confirm save.

☐ Provide the BOOTP server with the following data for a device:

```
# /etc/bootptab for BOOTP-daemon bootpd
#
# gw -- gateway
# ha -- hardware address
# ht -- hardware type
# ip -- IP address
# sm -- subnet mask
# tc -- template

.global:\
:gw=0.0.0.0:\
:sm=255.255.240.0:
```

```
switch_01:ht=ethernet:ha=008063086501:ip=10.1.112.83:tc=.global:
switch_02:ht=ethernet:ha=008063086502:ip=10.1.112.84:tc=.global:
.
.
```

Lines that start with a '#' character are comment lines.

The lines under ".global:" make the configuration of several devices easier. With the template (tc) you allocate the global configuration data (tc=.global:) to each device .
The direct allocation of hardware address and IP address is performed in the device lines (switch-0...).

☐ Enter one line for each device.
☐ After ha= enter the hardware address of the device.
☐ After ip= enter the IP address of the device.

In the appendix under "Setting up a DHCP/BOOTP Server" on page 190, you will find an example for the configuration of a BOOTP/DHCP server.

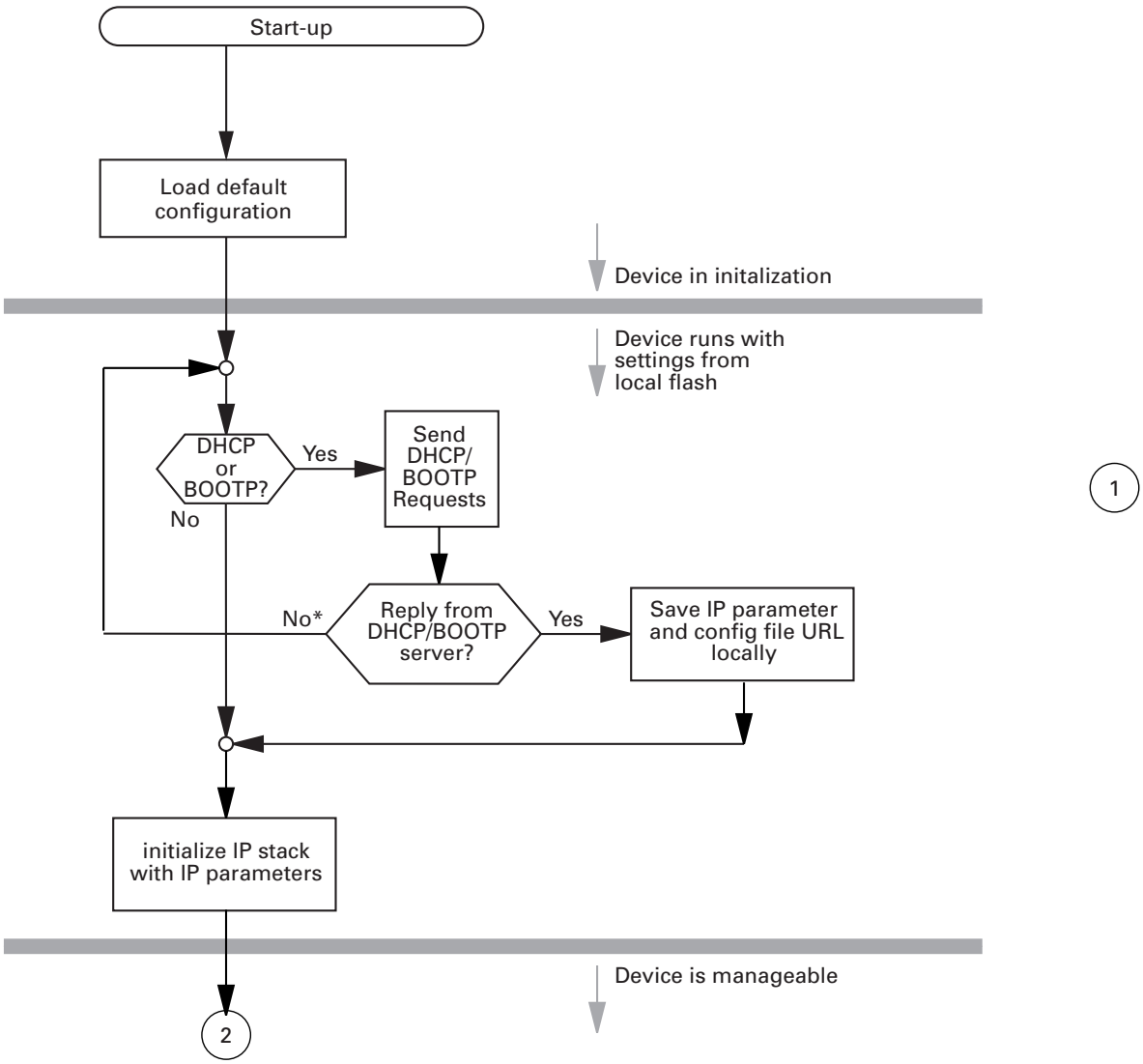


Figure 13: Flow chart for the BOOTP/DHCP process, part 1
** see fig. 14*

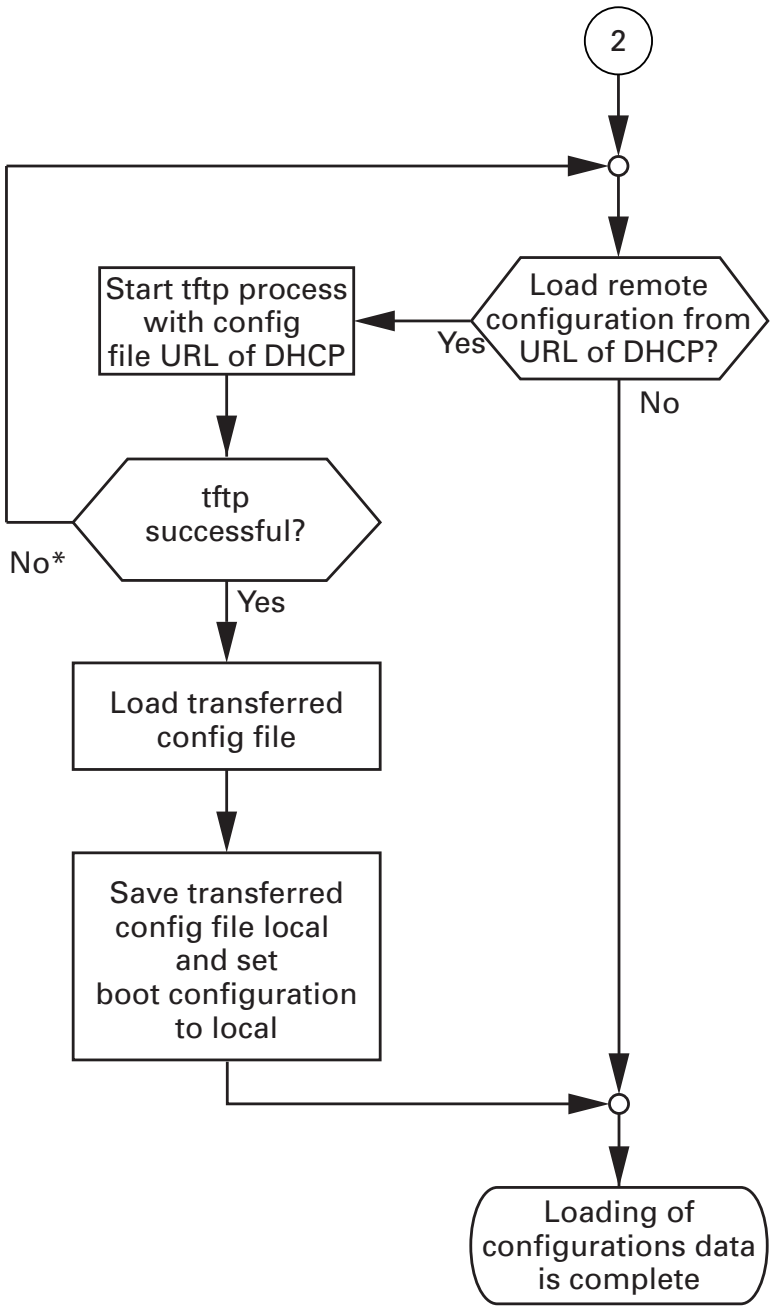

2
Load remote configuration from URL of DHCP?
Yes
Start tftp process with config file URL of DHCP
No
tftp successful?
No*
Yes
Load transferred config file
Save transferred config file local and set boot configuration to local
Loading of configurations data is complete

Figure 14: Flow chart for the BOOTP/DHCP process, part 2

Note: The loading process started by DHCP/BOOTP (see on page 190 “Setting up a DHCP/BOOTP Server“) shows the selection of "from URL & save locally" in the "Load" frame. If you get an error message when saving a configuration, this could be due to an active loading process. DHCP/BOOTP only finishes a loading process when a valid configuration has been loaded. If DHCP/BOOTP does not find a valid configuration, then finish the loading process by loading the local configuration in the "Load" frame.

2.6 System Configuration via DHCP

The DHCP (Dynamic Host Configuration Protocol) is a further development of BOOTP, which it has replaced. The DHCP additionally allows the configuration of a DHCP client via a name instead of via the MAC address. For the DHCP, this name is known as the “client identifier” in accordance with rfc 2131.
The device uses the name entered under sysName in the system group of the MIB II as the client identifier. You can enter this system name directly via SNMP, the Web-based management (see system dialog), or the Command Line Interface.

During startup operation, a device receives its configuration data according to the “DHCP process” flowchart (see fig. 13).

The device sends its system name to the DHCP server. The DHCP server can then use the system name to allocate an IP address as an alternative to the MAC address.
In addition to the IP address, the DHCP server sends
– the netmask
– the default gateway (if available)
– the tftp URL of the configuration file (if available).

The device accepts this data as configuration parameters (see on page 48 “Web-based IP Configuration“).
If an IP address was assigned by a DHCP server, it will be permanently saved locally.

Option	Meaning
1	Subnet Mask
2	Time Offset
3	Router
4	Time server
12	Host Name
61	Client Identifier
66	TFTP Server Name
67	Bootfile Name

Table 3: DHCP options which the device requests

The advantage of using DHCP instead of BOOTP is that the DHCP server can restrict the validity of the configuration parameters (“Lease”) to a specific time period (known as dynamic address allocation). Before this period (“Lease Duration”) elapses, the DHCP client can attempt to renew this lease. Alternatively, the client can negotiate a new lease. The DHCP server then allocates a random free address.
To avoid this, most DHCP servers provide the explicit configuration option of always assigning a specific client the same IP address based on a unique hardware ID (known as static address allocation).

On delivery, DHCP is activated.
As long as DHCP is activated, the device attempts to obtain an IP address. If it cannot find a DHCP server after restarting, it will not have an IP address.
To activate/deactivate DHCP (see on page 48 “Web-based IP Configuration“).

Note: When using HiVision network management, ensure that DHCP always allocates the original IP address to each device.

In the appendix, you will find an example for the configuration of a BOOTP/DHCP server (see on page 190 “Setting up a DHCP/BOOTP Server“).

Example of a DHCP configuration file:

```
# /etc/dhcpd.conf for DHCP Daemon
#
subnet 10.1.112.0 netmask 255.255.240.0 {
option subnet-mask 255.255.240.0;
option routers 10.1.112.96;
}
#
# Host berta requests IP configuration
# with her MAC address
#
host berta {
hardware ethernet 00:80:63:08:65:42;
fixed-address 10.1.112.82;
}
#
# Host hugo requests IP configuration
# with his client identifier.
#
host hugo {
#
option dhcp-client-identifier "hugo";
option dhcp-client-identifier 00:68:75:67:6f;
fixed-address 10.1.112.83;
server-name "10.1.112.11";
filename "/agent/config.dat";
}
```

Lines that start with a '#' character are comment lines.
The lines preceding the individually listed devices refer to settings that apply to all the following devices.
The fixed-address line assigns a permanent IP address to the device.
For further information, please refer to the DHCP server manual.

2.7 System Configuration via DHCP Option 82

As with the classic DHCP, on startup an agent receives its configuration data according to the “BOOTP/DHCP process” flow chart (see fig. 13).

While the system configuration is based on the classic DHCP protocol on the device being configured (see on page 44 “System Configuration via DHCP“), Option 82 is based on the network topology. This procedure gives you the option of always assigning the same IP address to any device which is connected to a particular location (port of a device) on the LAN.
The installation of a DHCP server is described in the chapter “Setting up a DHCP Server with Option 82“ on page 196.

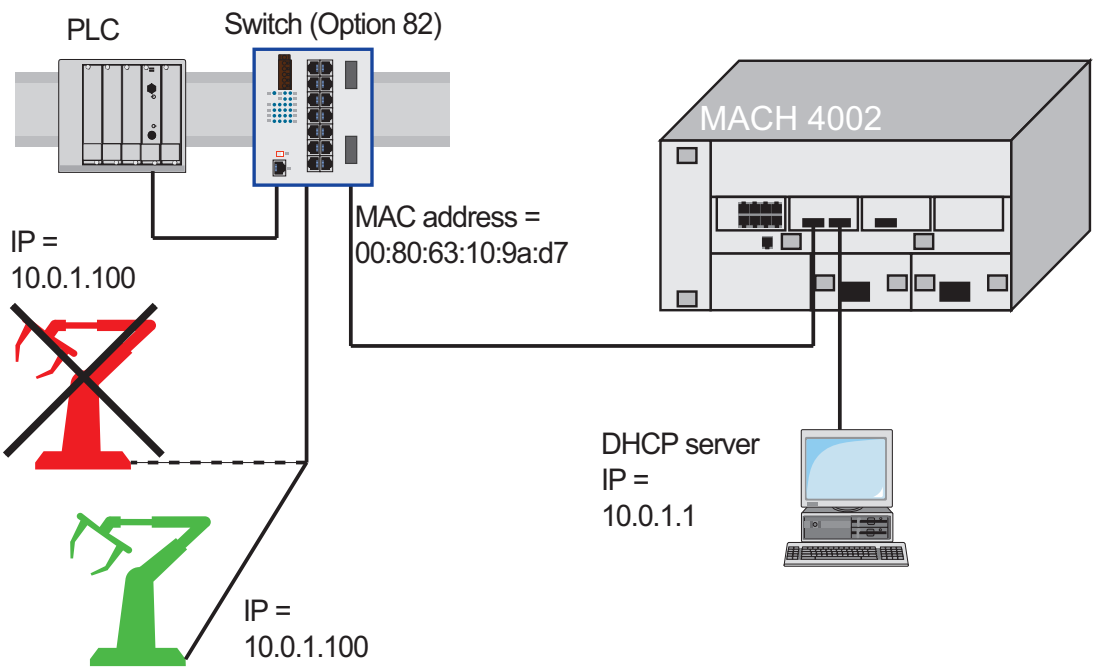


Figure 15: Application example of using Option 82

2.8 Web-based IP Configuration

With the `Basic Settings:Network` dialog you define the source from which the device gets its IP parameters after starting, and you assign the IP parameters and VLAN ID and configure the HiDiscovery access.

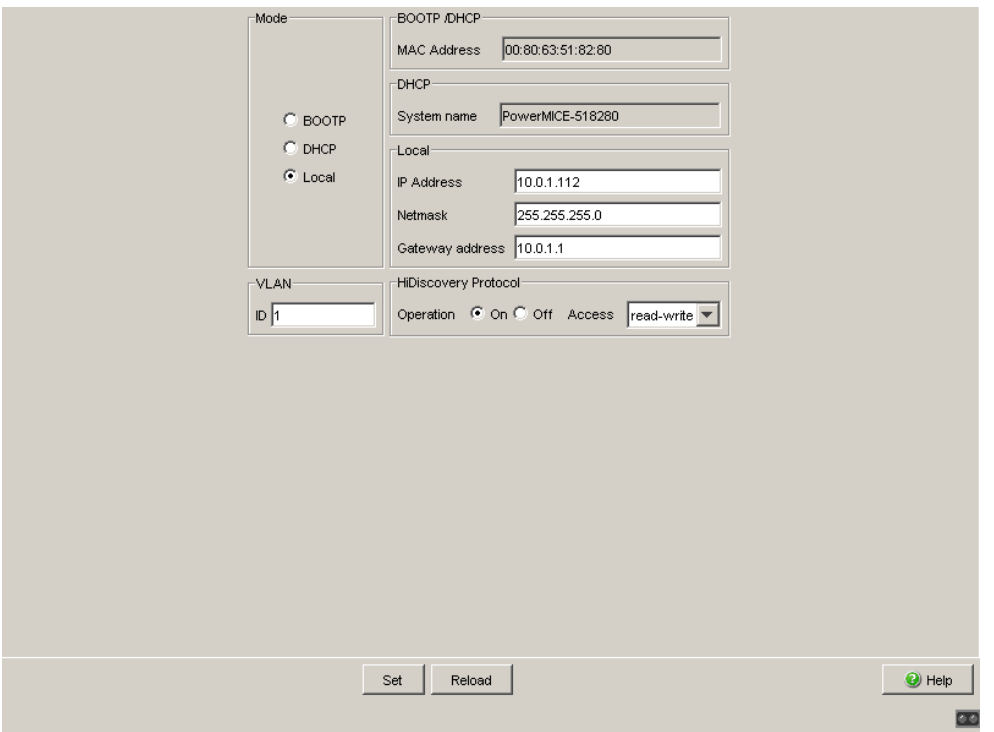


Figure 16: Network Parameters Dialog

☐ Under “Mode”, you enter where the device gets its IP parameters:
- In the BOOTP mode, the configuration is via a BOOTP or DHCP server on the basis of the MAC address of the device (see page 190 “Setting up a DHCP/BOOTP Server“).
- In the DHCP mode, the configuration is via a DHCP server on the basis of the MAC address or the name of the device (see page 196 “Setting up a DHCP Server with Option 82“).
- In the “local” mode the net parameters in the device memory are used.

☐ Enter the parameters on the right according to the selected mode.

☐ You enter the name applicable to the DHCP protocol in the “Name” line in the system dialog of the Web-based interface.

☐ The “VLAN” frame enables you to assign a VLAN to the agent. If you enter 0 here as the VLAN ID (not included in the VLAN standard version), the agent will then be accessible from all VLANs.

☐ The HiDiscovery protocol allows you to allocate an IP address to the device on the basis of its MAC address. Activate the HiDiscovery protocol if you want to allocate an IP address to the device from your PC with the enclosed HiDiscovery software (state on delivery: operation “on”, access “read-write”).

Note: Save the settings so that you will still have the entries after a restart (see on page 51 “Loading/saving settings“).

2.9 Faulty Device Replacement

The device provides 2 plug-and-play solutions for replacing a faulty device with a device of the same type (faulty device replacement):

- Configuring the new device using an AutoConfiguration Adapter(see on page 37 “Loading the system configuration from the ACA“) or
- configuration via DHCP Option 82 (see on page 196 “Setting up a DHCP Server with Option 82“)

In both cases, when the new device is started, it is given the same configuration data that the replaced device had.

Note: If you replace a device with DIP switches, please ensure that the DIP switch settings are identical.

3 Loading/saving settings

The device saves settings such as the IP parameters and the port configuration in the temporary memory. These settings are lost when you switch off orreboot the device.
The device enables you to

- load settings from a non-volatile memory into the temporary memory
- save settings from the temporary memory in a non-volatile memory.

If you change the current configuration (for example, by switching a port off), the Web-based interface changes the “load/save” symbol in the navigation tree from a disk symbol to a yellow triangle. After saving the configuration, the Web-based interface displays the “load/save” symbol as a disk again.

3.1 Loading settings

When it is restarted, the device loads its configuration data from the local non-volatile memory, provided you have not activated BOOTP/DHCP and no ACA is connected to the device.

During operation, the device allows you to load settings from the following sources:

- the local non-volatile memory
- from the AutoConfiguration Adapter. If an ACA is connected to the device, the device automatically loads its configuration from the ACA during the boot procedure.
- a file in the connected network (setting on delivery)
- a binary file and
- the firmware (restoration of the configuration on delivery).

Note: When loading a configuration, do not access the device until it has loaded the configuration file and has made the new configuration settings. Depending on the complexity of the configuration settings, this procedure may take 10 to 200 seconds.

3.1.1 Loading from the local non-volatile memory

When loading the configuration data locally, the device loads the configuration data from the local non-volatile memory if no ACA is connected to the device.

☐ Select the `Basics: Load/Save` dialog.
☐ In the "Load" frame, click "from Device".
☐ Click "Restore".

`enable`	Switch to the Privileged EXEC mode.
`copy nvram:startup-config system:running-config`	The device loads the configuration data from the local non-volatile memory.

3.1.2 Loading from the AutoConfiguration Adapter

If a ACA is connected to the device, the device automatically loads its configuration from the ACA during the boot procedure.
The chapter “Saving locally (and on the ACA)“ on page 57 describes how to save a configuration file on an ACA.

Note: The device allows you to trigger the following events when the configuration stored on the ACA does not match that in the device:
- an alarm (trap) is sent (see on page 157 “Configuring Traps“),
- the device status is updated (see on page 159 “Monitoring the Device Status“),
- the status of the signal contacts is updated (see on page 163 “Controlling the Signal Contact“).

3.1.3 Loading from a file

The device allows you to load the configuration data from a file in the connected network if there is no AutoConfiguration Adapter connected to the device.

☐ Select the `Basics: Load/Save` dialog.
☐ In the "Load" frame, click
- "from URL" if you want the device to load the configuration data from a file and retain the locally saved configuration.
- "from URL & save to Switch" if you want the device to load the configuration data from a file and save this configuration locally.
- "via PC" if you want the device to load the configuration data from a file from the PC and retain the locally saved configuration.

☐ In the "URL" frame, enter the path under which the device will find the configuration file, if you want to load from the URL.
☐ Click "Restore".

The URL identifies the path to the tftp server from which the device loads the configuration file. The URL is in the format tftp://IP address of the tftp server/path name/file name (e.g. `tftp://10.1.112.5/switch/config.dat`).

Example of loading from a tftp server
☐ Before downloading a file from the tftp server, you have to save the configuration file in the corresponding path of the tftp servers with the file name, e.g. `switch/switch_01.cfg` (see on page 58 “Saving to a file on URL“)
☐ In the "URL" line, enter the path of the tftp server, e.g. `tftp://10.1.112.214/switch/switch_01.cfg`.

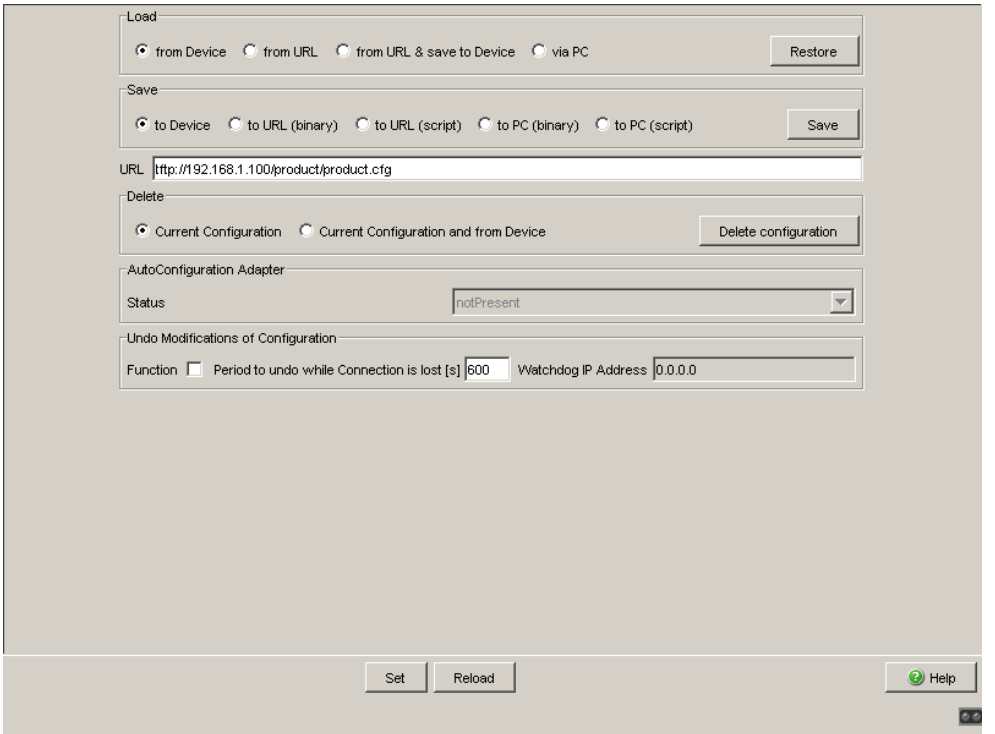


Figure 17: Load/Save dialog

```
enable
copy tftp://10.1.112.159/
switch/config.dat
nvram:startup-config
```

Switch to the Privileged EXEC mode.

The device loads the configuration data from a tftp server in the connected network.

Note: The loading process started by DHCP/BOOTP (see on page 39 “System configuration via BOOTP“) shows the selection of "from URL & save locally" in the "Load" frame. If you get an error message when saving a configuration, this could be due to an active loading process. DHCP/BOOTP only finishes a loading process when a valid configuration has been loaded. If DHCP/BOOTP does not find a valid configuration, then finish the loading process by loading the local configuration in the "Load" frame.

3.1.4 Resetting the configuration to the state on delivery

The device enables you to

- reset the current configuration to the state on delivery. The locally saved configuration is kept.
- reset the device to the state on delivery. After the next restart, the IP address is also in the state on delivery.

☐ Select the `Basics: Load/Save` dialog.
☐ Make your selection in the "Delete" frame.
☐ Click "Delete configuration".

Setting in the system monitor

☐ Select `5` “Erase main configuration file”
This menu item allows you to reset the device to its state on delivery. The device saves configurations other than the original one in its Flash memory in the configuration file `*.cfg`.
☐ Press the Enter key to delete the configuration file.

3.2 Saving settings

In the "Save" frame, you have the option to

- save the current configuration on the device
- save the current configuration in binary form in a file under the specified URL
- save the current configuration in binary form on the PC

3.2.1 Saving locally (and on the ACA)

The device allows you to save the current configuration data in the local non-volatile memory and the ACA.

☐ Select the `Basics: Load/Save` dialog.
☐ In the “Save” frame, click “to Device”.
☐ Click on “Save”.
The device saves the current configuration data in the local non-volatile memory and, if an ACA is connected, also in the ACA.

```
enable
copy system:running-config
  nvram:startup-config
```

Switch to the Privileged EXEC mode.
The device saves the current configuration data in the local non-volatile memory and, if an ACA is connected, also on the ACA.

Note: After you have successfully saved the configuration on the device, the device sends an alarm (trap) `hmConfigurationSavedTrap` together with the information about the AutoConfiguration Adapter (ACA), if one is connected. When you change the configuration for the first time after saving it, the device sends a trap `hmConfigurationChangedTrap`.

Note: The device allows you to trigger the following events when the configuration stored on the ACA does not match that in the device:

- an alarm (trap) is sent (see on page 157 “Configuring Traps“),
- the device status is updated (see on page 160 “Configuring the Device Status“),
- the status of the signal contacts is updated (see on page 163 “Controlling the Signal Contact“).

3.2.2 Saving to a file on URL

The device allows you to save the current configuration data in a file in the connected network.

Note: The configuration file includes all configuration data, including the password. Therefore pay attention to the access rights on the tftp server.

☐ Select the
`Basics: Load/Save` dialog.
☐ In the “Save” frame, click “to URL (binary)”
to receive a binary file, or “to URL (script)”
to receive an editable and readable script.
☐ In the “URL” frame, enter the path under which you want the device to save the configuration file.

The URL identifies the path to the tftp server on which the device saves the configuration file. The URL is in the format
tftp://IP address of the tftp server/path name/file name
(e.g. `tftp://10.1.112.5/switch/config.dat`).

☐ Click "Save".

`enable`	Switch to the Privileged EXEC mode.
`copy nvram:startup-config tftp://10.1.112.159/ switch/config.dat`	The device saves the configuration data in a binary file on a tftp server in the connected network
`copy nvram:script tftp://10.0.1.159/switch/ config.txt`	The device saves the configuration data in a script file on a tftp server in the connected network.

4 Loading Software Updates

Hirschmann never stops working on improving the performance of its products. So it is possible that you may find a more up to date release of the device software on the Hirschmann Internet site (www.hirschmann.com) than the release saved on your device.

Checking the installed software release

- ☐ Select the `Basics:Software` dialog.
- ☐ This dialog shows you the variant, the release number and the date of the software saved on the device.
  - ▶ “Stored Version”: the software in the non-volatile memory
  - ▶ “Running Version”: the software currently being used
  - ▶ “Backup Version”: the backup software in the non-volatile memory

```
enable                                  Switch to the Privileged EXEC mode.
show sysinfo                            Display the system information.

Alarm..................................... None

System Description........................ Hirschmann Railswitch
System Name............................... RS-1F1054
System Location........................... Hirschmann Railswitch
System Contact............................ Hirschmann Automation
  and Control GmbH
System Up Time............................ 0 days 0 hrs 45 mins
  57 secs
System Date and Time (local time zone)..... 2009-11-12 14:15:16
System IP Address......................... 10.0.1.13
Boot Software Release..................... L2B-05.2.00
Boot Software Build Date.................. 2009-11-12 13:14
OS Software Release....................... L2B-03.1.00
OS Software Build Date.................... 2009-11-12 13:14
Hardware Revision......................... 1.22 / 4 / 0103
Hardware Description...................... RS20-1600T1T1SDAEHH
Serial Number............................. 943434023000001191
Base MAC Address.......................... 00:80:63:1F:10:54
Number of MAC Addresses................... 32 (0x20)
```

Loading the software

The device gives you 4 options for loading the software:

- manually from the ACA 21 USB (out-of-band),
- automatically from the ACA 21 USB (out-of-band),
- via TFTP from a tftp server (in-band) and
- via a file selection dialog from your PC.

Note: The existing configuration of the device is still there after the new software is installed.

4.1 Loading the Software manually from the ACA

You can connect the ACA 21-USB to a USB port of your PC like a conventional USB stick and copy the device software into the main directory of the ACA 12-USB.

☐ Connect the ACA 21-USB onto which you copied the device software with the USB port of the device.

☐ Open the system monitor (see page 14 “Opening the system monitor“).

☐ Select 2 and press the Enter key to copy the software from the ACA 21-USB into the local memory of the device. At the end of the update, the system monitor asks you to press any key to continue.

☐ Select 3 to start the new software on the device.

The system monitor offers you additional options in connection with the software on your device:

- selecting the software to be loaded
- starting the software
- performing a cold start

4.1.1 Selecting the software to be loaded

In this menu item of the system monitor, you select one of two possible software releases that you want to load.
The following window appears on the screen:

```
Select Operating System Image

(Available OS: Selected: 05.0.00 (2009-08-07 06:05), Backup: 04.2.00
 (2009-07-06 06:05 (Locally selected: 05.0.00 (2009-08-07 06:05))

1  Swap OS images
2  Copy image to backup
3  Test stored images in Flash mem.
4  Test stored images in USB mem.
5  Apply and store selection
6  Cancel selection
```

Figure 18: Update operating system screen display

- **Swap OS images**
  The memory of the device provides space for two images of the software. This gives you the ability to load a new version of the software without deleting the existing version.
  ☐ Select `1` to load the other software in the next booting process.

- **Copy image to backup**
  ☐ Select `2` to save a copy of the active software.

Test stored images in flash memory

☐ Select 3 to check whether the images of the software stored in the flash memory contain valid codes.

Test stored images in USB memory

☐ Select 4, to check whether the images of the software stored in the ACA 21-USB contain valid codes.

Apply and store selection

☐ Select 5 to confirm the software selection and to save it.

Cancel selection

☐ Select 6 to leave this dialog without making any changes.

4.1.2 Starting the software

This menu item (Start Selected Operating System) of the system monitor allows you to start the software selected.

4.1.3 Performing a cold start

This menu item (End (reset and reboot)) of the system monitor allows you to reset the hardware of the device and perform a restart.

4.2 Automatic software update by ACA

☐ For a software update via the ACA, first copy the new device software into the main directory of the AutoConfiguration Adapter. If the version of the software on the ACA is newer or older than the version on the device, the device performs a software update.

Note: Software versions with release 06.0.00 and higher in the non-volatile memory of the device support the software update via the ACA. If the device software is older, you have the option of loading the software manually from the ACA(see page 63).

☐ Give the file the name that matches the device type and the software variant, e.g. rsL2P.bin for device type RS2 with the software variant L2P. Please note the case-sensitivity here.
If you have copied the software from a CD-ROM or from a Web server of the manufacturer, the software already has the correct file name.

☐ Also create an empty file with the name “autoupdate.txt” in the main directory of the ACA. Please note the case-sensitivity here.

☐ Connect the AutoConfiguration Adapter to the device and restart the device.

☐ The device automatically performs the following steps:
- During the booting process, it checks whether an ACA is connected.
- It checks whether the ACA has a file with the name “autoupdate.txt” in the main directory.
- It checks whether the ACA has a software file with a name that matches the device type in the main directory.
- If compares the software version stored on the ACA with the one stored on the device.
- If these conditions are fulfilled, the device loads the software from the ACA to its non-volatile memory as the main software.
- The device then performs a cold start, during which it loads the new software from the non-volatile memory.

One of the following messages in the log file indicates the result of the update process:

- S_watson_AUTOMATIC_SWUPDATE_SUCCESSFUL: Update completed successfully.
- S_watson_AUTOMATIC_SWUPDATE_FAILED_WRONG_FILE: Update failed. Reason: incorrect file.
- S_watson_AUTOMATIC_SWUPDATE_FAILED_SAVING_FILE: Update failed. Reason: error when saving.

☐ In your browser, click on “Reload” so that you can use the Web-based interface to access the device again after it is booted.

4.3 Loading the software from the tftp server

For a tftp update, you need a tftp server on which the software to be loaded is stored (see on page 200 “TFTP Server for Software Updates“).

☐ Select the `Basics:Software` dialog.

The URL identifies the path to the software stored on the tftp server. The URL is in the format
tftp://IP address of the tftp server/path name/file name
(e.g. `tftp://192.168.1.1/device/device.bin`).

☐ Enter the path of the device software.

☐ Click on "Update" to load the software from the tftp server to the device.

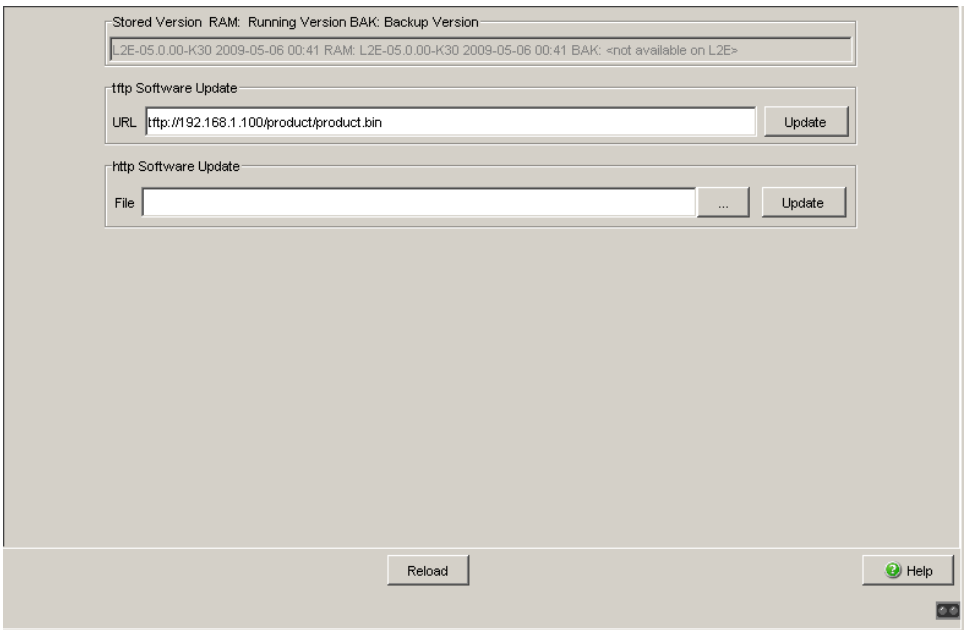


Figure 19: Software update dialog

☐ After successfully loading it, you activate the new software: Select the dialog `Basic Settings:Restart` and perform a cold start. In a cold start, the device reloads the software from the non-volatile memory, restarts, and performs a self-test.

☐ After booting the device, click "Reload" in your browser to access the device again.

`enable`	Switch to the Privileged EXEC mode.
`copy tftp://10.0.1.159/ rsL2E.bin system:image`	Transfer the "rsL2E.bin" software file to the device from the tftp server with the IP address 10.0.1.159.

4.4 Loading the Software via File Selection

For an HTTP software update (via a file selection window), the device software must be on a data carrier that you can access via a file selection window from your workstation.

- ☐ Select the `Basics:Software` dialog.
- ☐ In the file selection frame, click on “...”.
- ☐ In the file selection window, select the device software (name type: *.bin, e.g. device.bin) and click on “Open”.
- ☐ Click on “Update” to transfer the software to the device.

The end of the update is indicated by one of the following messages:

- ▶ Update completed successfully.
- ▶ Update failed. Reason: incorrect file.
- ▶ Update failed. Reason: error when saving.
- ▶ File not found (reason: file name not found or does not exist).
- ▶ Connection error (reason: path without file name).

- ☐ After the update is completed successfully, you activate the new software:
  Select the `Basic settings: Restart` dialog and perform a cold start.
  In a cold start, the device reloads the software from the non-volatile memory, restarts, and performs a self-test.
- ☐ In your browser, click on “Reload” so that you can access the device again after it is booted.

5 Configuring the Ports

The port configuration consists of:

- Switching the port on and off
- Selecting the operating mode
- Activating the display of connection error messages
- Configuring Power over ETHERNET.

Switching the port on and off

In the state on delivery, all the ports are switched on. For a higher level of access security, switch off the ports at which you are not making any connection.

☐ Select the `Basics:Port Configuration` dialog.
☐ In the "Port on" column, select the ports that are connected to another device.

Selecting the operating mode

In the state on delivery, all the ports are set to the “Automatic configuration” operating mode.

Note: The active automatic configuration has priority over the manual configuration.

☐ Select the `Basics:Port Configuration` dialog.
☐ If the device connected to this port requires a fixed setting
  – select the operating mode (transmission rate, duplex mode) in the "Manual configuration" column and
  – deactivate the port in the "Automatic configuration" column.

Displaying connection error messages

In the state on delivery, the device displays connection errors via the signal contact and the LED display. The device allows you to suppress this display, because you do not want to interpret a switched off device as an interrupted connection, for example.

- ☐ Select the `Basics:Port Configuration` dialog.
- ☐ In the "Propagate connection error" column, select the ports for which you want to have link monitoring.

Configuring Power over ETHERNET

Devices with Power over ETHERNET (PoE) media modules or PoE ports enable you to supply current to terminal devices such as IP phones via the twisted-pair cable. PoE media modules and PoE ports support Power over ETHERNET according to IEEE 802.3af.
On delivery, the Power over ETHERNET function is activated globally and at all ports.

Nominal power for MS20/30, MACH 1000 and PowerMICE:
The device provides the nominal power for the sum of all PoE ports plus a surplus. Because the PoE media module gets its PoE voltage externally, the device does not know the possible nominal power.
The device therefore assumes a “nominal power” of 60 Watt per PoE media module for now.

Nominal power for HS600x:
The device provides the nominal power for the sum of all PoE ports plus a surplus. Because the PoE media module gets its PoE voltage externally, the device does not know the possible nominal power.
The device therefore assumes a “nominal power” of 60 Watts per PoE media module for now.

Nominal power for OCTOPUS 8M-PoE:
The device provides the nominal power for the sum of all PoE ports plus a surplus. Because the device gets its PoE voltage externally, the device does not know the possible nominal power.
The device therefore assumes a “nominal power” of 15 Watt per PoE port for now.

- ☐ Select the `Basics:Power over Ethernet` dialog.
- ☐ With “Function on/off” you turn the PoE on or off.
- ☐ With “Send Trap” you can get the device to send a trap in the following cases:
  - – If a value exceeds/falls below the performance threshold.
  - – If the PoE supply voltage is switched on/off at at least one port.
- ☐ Enter the power threshold in “Threshold”. When this value is exceeded/not achieved, the device will send a trap, provided that “Send trap” is enabled. For the power threshold you enter the power yielded as a percentage of the nominal power.
- ☐ “Nominal Power” displays the power that the device nominally provides for all PoE ports together.
- ☐ “Reserved Power” displays the maximum power that the device provides to all the connected PoE devices together on the basis of their classification.
- ☐ “Delivered Power” shows how large the current power requirement is at all PoE ports.

The difference between the "nominal" and "reserved" power indicates how much power is still available to the free PoE ports.

- ☐ In the “POE on” column, you can enable/disable PoE at this port.
- ☐ The “Status” column indicates the PoE status of the port.
- ☐ The “Class” column shows the class of the connected device:
  ClassMaximum power delivered
  0: 15.4 W = state on delivery
  1: 4.0 W
  2: 7.0 W
  3: 15,4 W
  4: reserved, treat as class 0
- ☐ The “Name” column indicates the name of the port, see `Basic settings:Port configuration`.

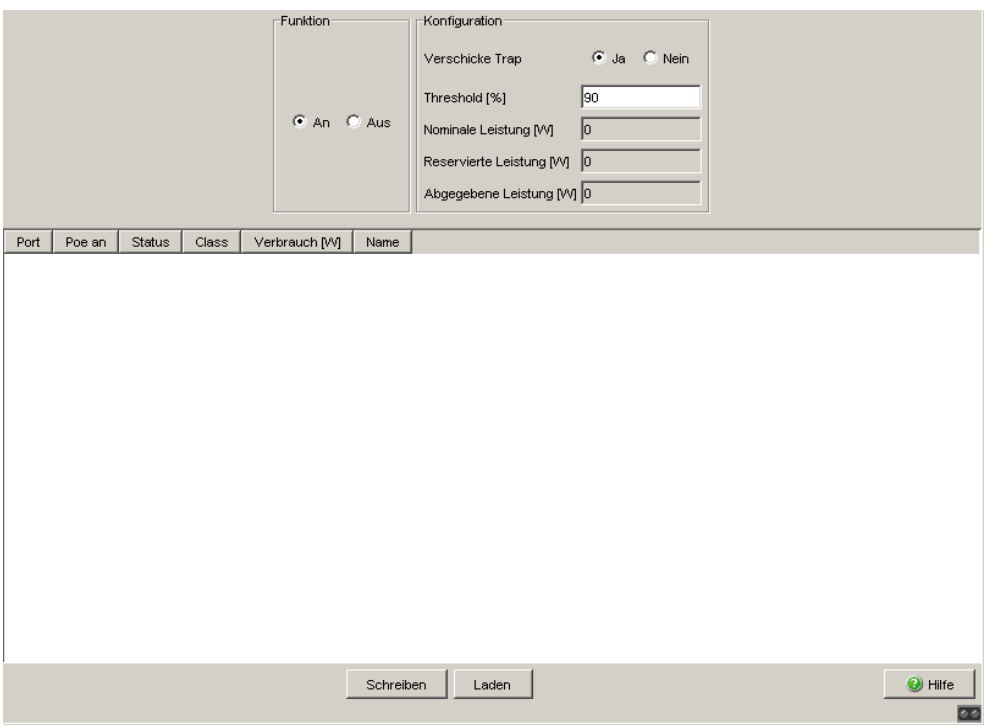


Figure 20: Power over Ethernet dialog

6 Protection from Unauthorized Access

The device provides you with the following functions to help you protect it against unauthorized access.

- Password for SNMP access
- Telnet/Web access disabling
- Restricted management access
- HiDiscovery function disabling
- Port access control via IP or MAC address

6.1 Protecting the device

If you want to maximize the protection of the device against unauthorized access in just a few steps, you can perform some or all of the following steps on the device:

- ☐ Deactivate SNMPv1 and SNMPv2 and select a password for SNMPv3 access other than the standard password (see on page 78 “Entering the password for SNMP access“).
- ☐ Deactivate Telnet access.
  Deactivate web access after you have downloaded the applet for the web-based interface onto your management station. You can start the web-based interface as an independent program and thus have SNMP access to the device (see on page 82 “Enabling/disabling Telnet/Web Access“).
- ☐ Deactivate HiDiscovery access.

Note: Make sure to retain at least one option to access the device. V.24 access is always possible, since it cannot be deactivated.

6.2 Password for SNMP access

6.2.1 Description of password for SNMP access

A network management station communicates with the device via the Simple Network Management Protocol (SNMP).
Every SNMP packet contains the IP address of the sending computer and the password with which the sender of the packet wants to access the device MIB.

The device receives the SNMP packet and compares the IP address of the sending computer and the password with the entries in the device MIB.
If the password has the appropriate access right, and if the IP address of the sending computer has been entered, then the device will allow access.

In the delivery state, the device is accessible via the password "public" (read only) and "private" (read and write) to every computer.

To help protect your device from unwanted access:

- ☐ First define a new password with which you can access from your computer with all rights.
- ☐ Treat this password as confidential, because everyone who knows the password can access the device MIB with the IP address of your computer.
- ☐ Limit the access rights of the known passwords or delete their entries.

6.2.2 Entering the password for SNMP access

☐ Select the `Security:Password/SNMP Access` dialog.
This dialog gives you the option of changing the read and read/write passwords for access to the device via the Web-based interface, via the CLI, and via SNMPv3 (SNMP version 3). Please note that passwords are case-sensitive.
Set different passwords for the read password and the read/write password so that a user that only has read access (user name “user”) does not know, or cannot guess, the password for read/write access (user name “admin”).
If you set identical passwords, when you attempt to write this data the device reports a general error.

The Web-based interface and the user interface (CLI) use the same passwords as SNMPv3 for the users “admin” and “user”.

☐ Select “Modify Read-Only Password (User)” to enter the read password.
☐ Enter the new read password in the “New Password” line and repeat your entry in the “Please retype” line.
☐ Select “Modify Read-Write Password (Admin)” to enter the read/write password.
☐ Enter the read/write password and repeat your entry.

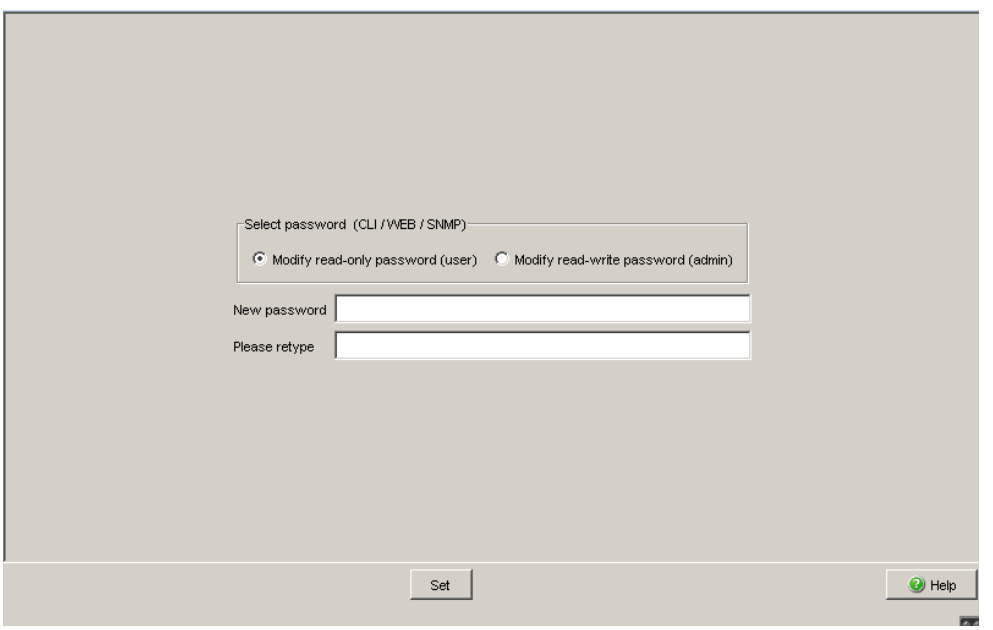


Figure 21: Password/SNMP Access dialog

Note: If you do not know a password with “read/write” access, you will not have write access to the device.

Note: For security reasons, the device does not display the passwords. Make a note of every change. You cannot access the device without a valid password.

Note: For security reasons, SNMPv3 encrypts the password. With the “SNMPv1” or “SNMPv2” setting in the dialog `Security:SNMPv1/v2 access`, the device transfers the password unencrypted, so that this can also be read.

Note: Use between 5 and 32 characters for the password in SNMPv3, since many applications do not accept shorter passwords.

☐ Select the Security:SNMPv1/v2 access dialog.
With this dialog you can select the access via SNMPv1 or SNMPv2. In the state on delivery, both protocols are activated. You can thus manage the device with HiVision and communicate with earlier versions of SNMP.

If you select SNMPv1 or SNMPv2, you can specify in the table via which IP addresses the device may be accessed, and what kinds of passwords are to be used.
Up to 8 entries can be made in the table.
For security reasons, the read password and the read/write password must not be identical.
Please note that passwords are case-sensitive.

Index	Serial number for this table entry
Password	Password with which this computer can access the device. This password is independent of the SNMPv2 password.
IP address	IP address of the computer that can access the device.
IP mask	IP mask for the IP address

Access mode	The access mode determines whether the computer has read-only or read-write access.
Active	Enable/disable this table entry.

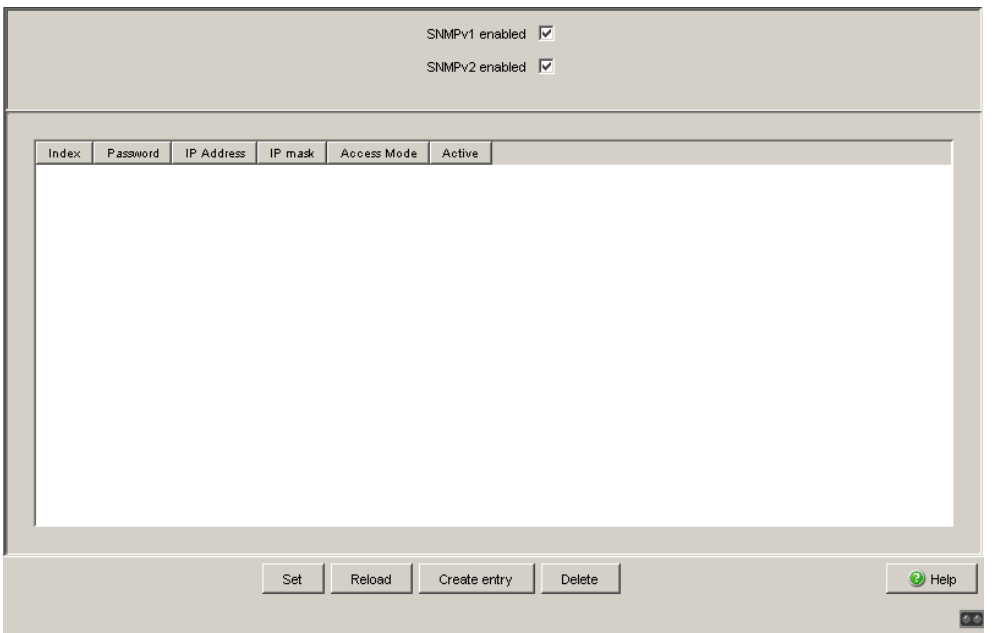


Figure 22: SNMPv1/v2 access dialog

☐ To create a new line in the table click "Create entry".
☐ To delete an entry, select the line in the table and click "Delete".

6.3 Telnet/Web Access

6.3.1 Description of Telnet Access

The Telnet server of the device allows you to configure the device by using the Command Line Interface (in-band). You can deactivate the Telnet server if you do not want Telnet access to the device.
On delivery, the server is activated.
After the Telnet server has been deactivated, you will no longer be able to access the device via a new Telnet connection. If a Telnet connection already exists, it is kept.

Note: The Command Line Interface (out-of-band) and the `Security:Telnet/Web access` dialog in the Web-based interface allow you to reactivate the Telnet server.

6.3.2 Description of Web Access

The Web server of the device allows you to configure the device by using the Web-based interface. Deactivate the Web server if you do not want the device to be accessed from the Web.
On delivery, the server is activated.

After the Web server has been switched off, it is no longer possible to log in via a Web browser. The login in the open browser window remains active.

6.3.3 Enabling/disabling Telnet/Web Access

☐ Select the `Security:Telnet/Web access` dialog.

☐ Disable the server to which you want to refuse access.

`enable`	Switch to the Privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`lineconfig`	Switch to the configuration mode for CLI.
`transport input telnet`	Enable Telnet server.
`no transport input telnet`	Disable Telnet server.
`exit`	Switch to the Configuration mode.
`ip http server`	Enable Web server.
`no ip http server`	Disable Web server.
`ip ssh`	Enable SSH function on Switch
`no ip ssh`	Disable SSH function on Switch

6.4 HiDiscovery Access

6.4.1 Description of the HiDiscovery Protocol

The HiDiscovery protocol allows you to allocate an IP address to the device on the basis of its MAC address (see on page 34 “Entering the IP Parameters via HiDiscovery“). HiDiscovery is a Layer 2 protocol.

Note: For security reasons, restrict the HiDiscovery function for the device or disable it after you have assigned the IP parameters to the device.

6.4.2 Enabling/disabling the HiDiscovery Function

☐ Select the `Basics:Network` dialog.

☐ Disable the HiDiscovery function in the "HiDiscovery Protocol" frame or limit the access to "read-only".

`enable`	Switch to the Privileged EXEC mode.
`network protocol hidiscovery off`	Disable HiDiscovery function.
`network protocol hidiscovery read-only`	Enable HiDiscovery function with "read-only" access
`network protocol hidiscovery read-write`	Enable HiDiscovery function with "read-write" access

d

6.4.3 Description of the Port Access Control

You can configure the device in such a way that it helps to protect every port from unauthorized access. Depending on your selection, the device checks the MAC address or the IP address of the connected device.
The following functions are available for monitoring every individual port:

- The device can distinguish between authorized and unauthorized access and supports two types of access control:
  - Access for all:
    – no access restriction.
    – MAC address 00:00:00:00:00:00 or
    – IP address 0.0.0.0.
  - Access exclusively for defined MAC and IP addresses:
    – only devices with defined MAC or IP addresses have access.
    – You can define up to 10 IP addresses, MAC addresses or maskable MAC addresses.
- The device can react to an unauthorized access attempt in 3 selectable ways:
  - none: no response
  - trapOnly: message by sending a trap
  - portDisable: message by sending a trap and disabling the port

6.4.4 Application Example for Port Access Control

You have a LAN connection in a room that is accessible to everyone. To set the device so that only defined users can use the LAN connection, activate the port access control on this port. An unauthorized access attempt will cause the device to shut down the port and alert you with an alarm message. The following is known:

Parameter	Value	Explanation
Allowed IP Addresses	10.0.1.228 10.0.1.229	The defined users are the device with the IP address 10.0.1.228 and the device with the IP address 10.0.1.229
Action	portDisable	Disable the port with the corresponding entry in the port configuration table (see on page 71 “Configuring the Ports“) and send an alarm

Prerequisities for further configuration:

- The port for the LAN connection is enabled and configured correctly (see on page 71 “Configuring the Ports“)
- Prerequisites for the device to be able to send an alarm (trap) (see on page 157 “Configuring Traps“):
  - You have entered at least one recipient
  - You have set the flag in the “Active” column for at least one recipient
  - In the “Selection” frame, you have selected “Port Security”

☐ Configure the port security.

☐ Select the `Security:Port Security` dialog.

☐ In the “Configuration” frame, select “IP-Based Port Security”.
☐ In the table, click on the row of the port to be protected, in the “Allowed IP addresses” cell.
☐ Enter in sequence:
– the IP subnetwork group: 10.0.1.228
– a space character as a separator
– the IP address: 10.0.1.229
Entry: `10.0.1.228 10.0.1.229`
☐ In the table, click on the row of the port to be protected, in the “Action” cell, and select `portDisable`.

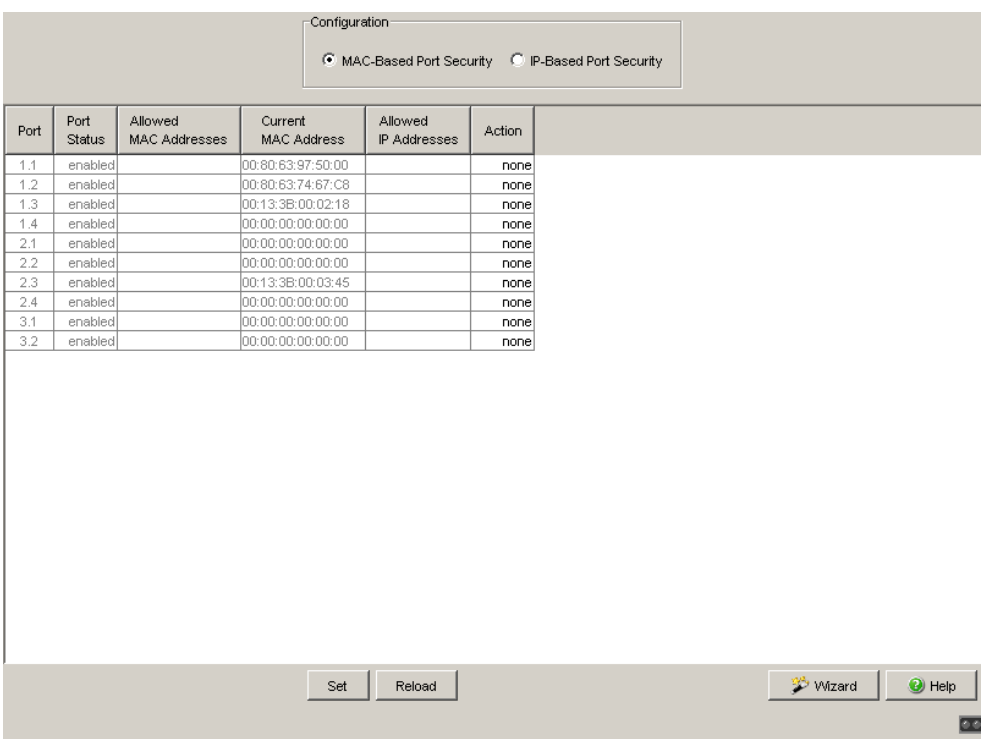


Figure 23: Port Security dialog

☐ Save the settings in the non-volatile memory.

☐ Select the dialog `Basic Settings:Load/Save`.
☐ In the “Save” frame, select “To Device” for the location and click “Save” to permanently save the configuration in the active configuration.

7 Synchronizing the System Time in the Network

The actual meaning of the term “real time” depends on the time requirements of the application.

The device provides two options with different levels of accuracy for synchronizing the time in your network.

If you only require an accuracy in the order of milliseconds, the Simple Network Time Protocol (SNTP) provides a low-cost solution. The accuracy depends on the signal runtime.

IEEE 1588 with the Precision Time Protocol (PTP) achieves accuracies in the order of fractions of microseconds. This superior method is suitable for process control, for example.

Examples of application areas include:
- log entries
- time stamping of production data
- production control, etc.

Select the method (SNMP or PTP) that best suits your requirements. You can also use both methods simultaneously if you consider that they interact.

7.1 Entering the Time

If no reference clock is available, you have the option of entering the system time in a device and then using it like a reference clock (see on page 94 “Configuring SNTP“).

Note: When setting the time in zones with summer and winter times, make an adjustment for the local offset. The device can also get the SNTP server IP address and the local offset from a DHCP server.

☐ Select the `Time` dialog.

With this dialog you can enter time-related settings independently of the time synchronization protocol selected.

- The “IEEE 1588 time” displays the time determined using PTP.
  The “SNTP time” displays the time with reference to Universal Time Coordinated (UTC).
  The display is the same worldwide. Local time differences are not taken into account.

- The “System time” uses the “IEEE 1588 / SNTP time”, allowing for the local time difference from “IEEE 1588 / SNTP time”.
  “System time” = “IEEE 1588 / SNTP time” + “Local offset”.
- “Time source” displays the source of the following time data. The device automatically selects the source with the greatest accuracy. Possible sources are: `local` and `sntp`. The source is initially `local`. If SNTP is activated and if the device receives a valid SNTP packet, the device sets its time source to `sntp`.

- With “Set time from PC”, the device takes the PC time as the system time and calculates the IEEE 1588 / SNTP time using the local time difference.
  “IEEE 1588 / SNTP time” = “System time” - “Local offset”
- The “Local Offset” is for displaying/entering the time difference between the local time and the “IEEE 1588 / SNTP time”.

  With “Set offset from PC”, the agent determines the time zone on your PC and uses it to calculate the local time difference.

`enable`	Switch to the Privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`sntp time <YYYY-MM-DD HH:MM:SS>`	Set the system time of the device.
`sntp client offset <-1000 to 1000>`	Enter the time difference between the local time and the "IEEE 1588 / SNTP time".

7.2 SNTP

7.2.1 Description of SNTP

The Simple Network Time Protocol (SNTP) enables you to synchronize the system time in your network.
The device supports the SNTP client and the SNTP server function.
The SNTP server makes the UTC (Universal Time Coordinated) available. UTC is the time relating to the coordinated world time measurement. The time displayed is the same worldwide. Local time differences are not taken into account.
The SNTP client obtains the UTC from the SNTP server.

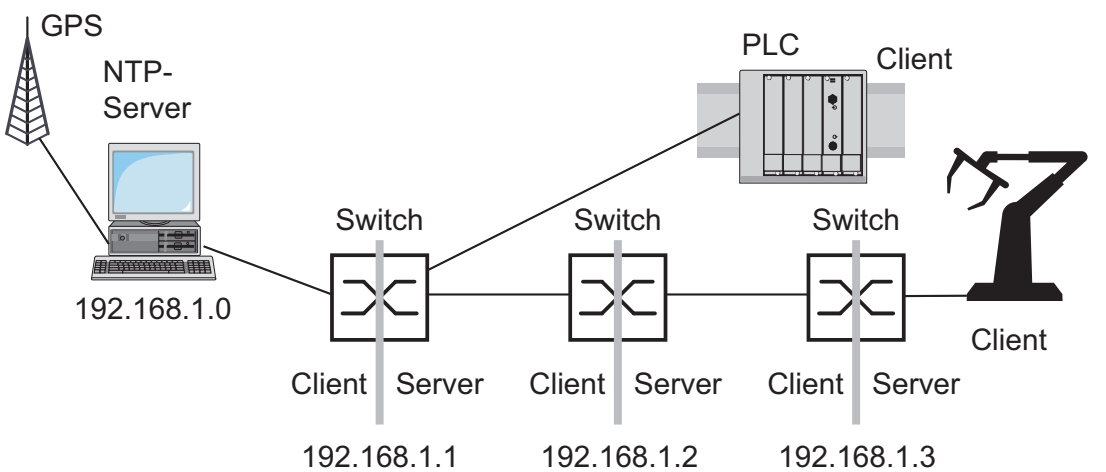


Figure 24: SNTP cascade

7.2.2 Preparing the SNTP Configuration

☐ To get an overview of how the time is passed on, draw a network plan with all the devices participating in SNTP. When planning, bear in mind that the accuracy of the time depends on the signal runtime.

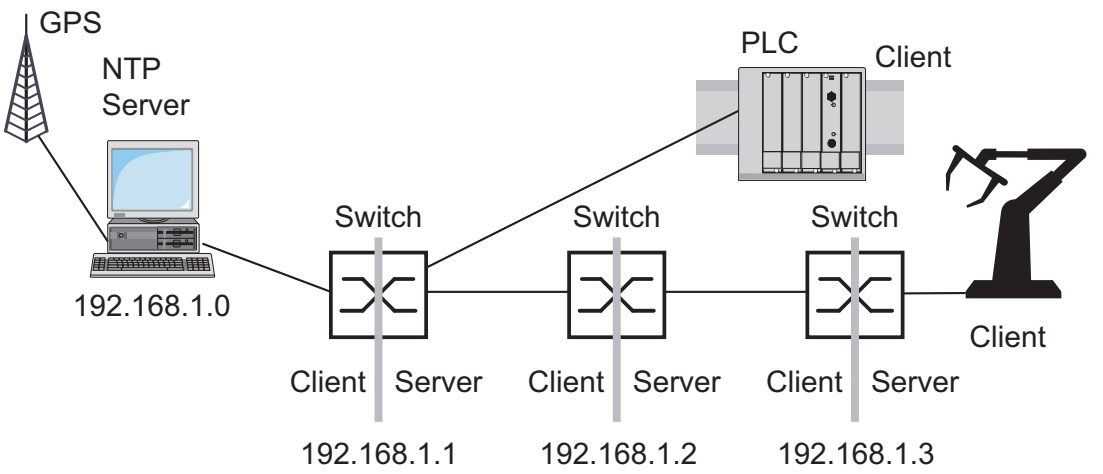


Figure 25: Example of SNTP cascade

☐ Enable the SNTP function on all devices whose time you want to set using SNTP.
The SNTP server of the device responds to Unicast requests as soon as it is enabled.

☐ If no reference clock is available, specify a device as the reference clock and set its system time as accurately as possible.

Note: For the most accurate system time distribution possible, only use network components (routers, switches, hubs) which support SNTP in the signal path between the SNTP server and the SNTP client.

7.2.3 Configuring SNTP

☐ Select the `Time:SNTP` dialog.

▶ Operation

☐ In this frame you switch the SNTP function on/off globally.

▶ SNTP Status

☐ The “Status message” displays statuses of the SNTP client as one or more test messages. Possible messages:

`Local system clock is synchronized; An SNTP loop has occurred; General error; Synchronized one time; Client deactivated; Server 1 is not synchronized; Server 1 has incorrect protocol version; Server 1 not responding; Server 2 is not synchronized; Server 2 has incorrect protocol version; Server 2 not responding.`

▶ Configuration SNTP Client

☐ In “Client status” you switch the SNTP client of the device on/off.

☐ In “External server address” you enter the IP address of the SNTP server from which the device periodically requests the system time.

☐ In “Redundant server address” you enter the IP address of the SNTP server from which the device periodically requests the system time, if it does not receive a response to a request from the “External server address” within 1 second.

Note: If you are receiving the system time from an external/ redundant server address, you do not accept any SNTP Broadcasts (see below). You thus ensure that the device uses the time of the server entered.

☐ In “Server request interval” you specify the interval at which the device requests SNTP packets (valid entries: 1 s to 3600 s, on delivery: 30 s).

☐ With “Accept SNTP Broadcasts” the device takes the system time from SNTP Broadcast/Multicast packets that it receives.

☐ With “Deactivate client after synchronization”, the device only synchronizes its system time with the SNTP server one time after the client status is activated, then it switches the client off.

Note: If you have enabled PTP at the same time, the SNTP client first collects 60 time stamps before it deactivates itself. The device thus determines the drift compensation for its PTP clock. With the preset server request interval, this takes about half an hour.

- Configuration SNTP Server
  - ☐ In “Server status” you switch the SNTP server of the device on/off.
  - ☐ In “Anycast destination address” you enter the IP address to which the SNTP server of the device sends its SNTP packets (see table 4).
  - ☐ In “VLAN ID” you specify the VLAN to which the device periodically sends its SNTP packets.
  - ☐ In “Anycast send interval” you specify the interval at which the device sends SNTP packets (valid entries: 1 s to 3,600 s, on delivery: 120 s).
  - ☐ With “Disable Server at local time source” the device disables the SNTP server function if the source of the time is `local` (see `Time` dialog).

IP destination address	Send SNTP packet to
0.0.0.0	Nobody
Unicast address (0.0.0.1 - 223.255.255.254)	Unicast address
Multicast address (224.0.0.0 - 239.255.255.254), especially 224.0.1.1 (NTP address)	Multicast address
255.255.255.255	Broadcast address

Table 4: Destination address classes for SNTP packets

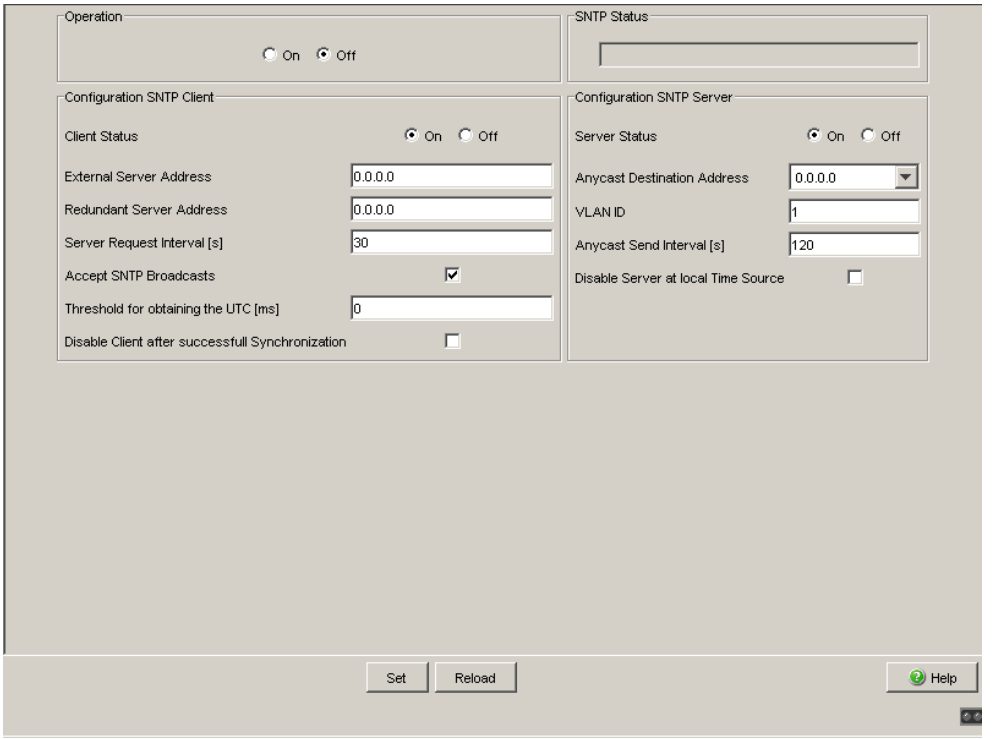


Figure 26: SNTP Dialog

Device	192.168.1.1	192.168.1.2	192.168.1.3
Operation	On	On	On
Server destination address	0.0.0.0	0.0.0.0	0.0.0.0
Server VLAN ID	1	1	1
Send interval	120	120	120
Client external server address	192.168.1.0	192.168.1.1	192.168.1.2
Request interval	30	30	30
Accept Broadcasts	No	No	No

Table 5: Settings for the example (see fig. 25)

7.3 Precision Time Protocol

7.3.1 Description of PTP Functions

Precise time management is required for running time-critical applications via a LAN.
The IEEE 1588 standard with the Precision Time Protocol (PTP) describes a procedure that assumes one clock is the most accurate and thus enables precise synchronization of all clocks in a LAN.

This procedure enable the synchronization of the clocks involved to an accuracy of a few 100 ns. The synchronization messages have virtually no effect on the network load. PTP uses Multicast communication.

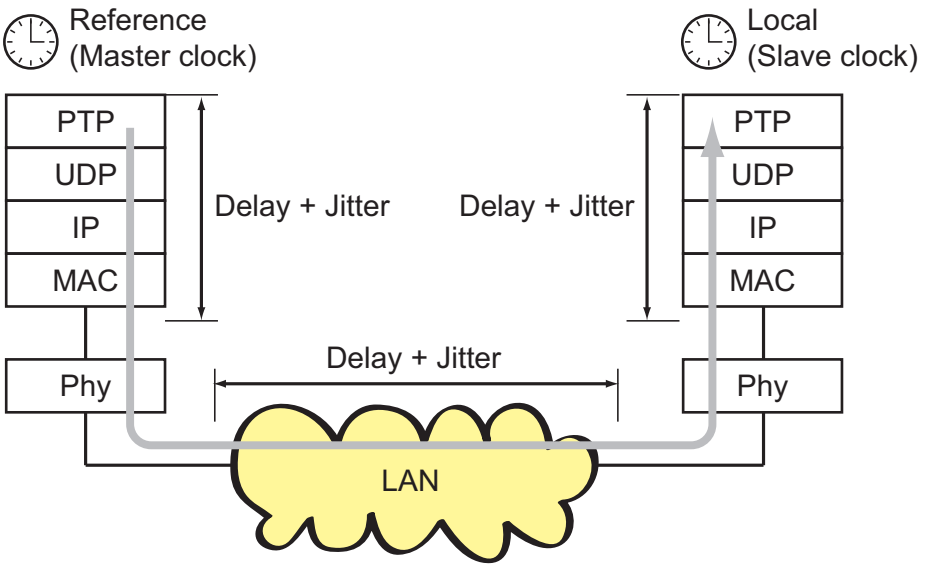
Factors influencing precision are:

- Accuracy of the reference clock
  IEEE 1588 classifies clocks according to their accuracy. An algorithm that measures the accuracy of the clocks available in the network specifies the most accurate clock as the "Grandmaster" clock.

PTPv1 Stratum number	PTPv2 Clock class	Specification
0	– (priority 1 = 0)	For temporary, special purposes, in order to assign a higher accuracy to one clock than to all other clocks in the network.
1	6	Indicates the reference clock with the highest degree of accuracy. The clock can be both a boundary clock and an ordinary clock. Stratum 1/ clock class 6 clocks include GPS clocks and calibrated atomic clocks. A stratum 1 clock cannot be synchronized using the PTP from another clock in the PTP system.
2	6	Indicates the second-choice reference clock.
3	187	Indicates the reference clock that can be synchronized via an external connection.
4	248	Indicates the reference clock that cannot be synchronized via an external connection. This is the standard setting for boundary clocks.
5–254	–	Reserved.
255	255	Such a clock should never be used as the best master clock.

Table 6: Stratum – classifying the clocks

- Cable delays; device delays
  The communication protocol specified by IEEE 1588 enables delays to be determined. Formulas for calculating the current time eliminate delays.
- Accuracy of local clocks
  The communication protocol specified by IEEE 1588 takes into account the inaccuracy of local clocks in relation to the reference clock. Calculation formulas permit the synchronization of the local time, taking into account the inaccuracy of the local clock in relation to the reference clock.



PTP	Precision Time Protocol (Application Layer)
UDP	User Datagramm Protocol (Transport Layer)
IP	Internet Protocol (Network Layer)
MAC	Media Access Control
Phy	Physical Layer

Figure 27: Delay and jitter for clock synchronization

Independently of the physical communication paths, the PTP provides logical communication paths which you define by setting up PTP subdomains. Subdomains are used to form groups of clocks that are time-independent from the rest of the domain. Typically, the clocks in a group use the same communication paths as other clocks.

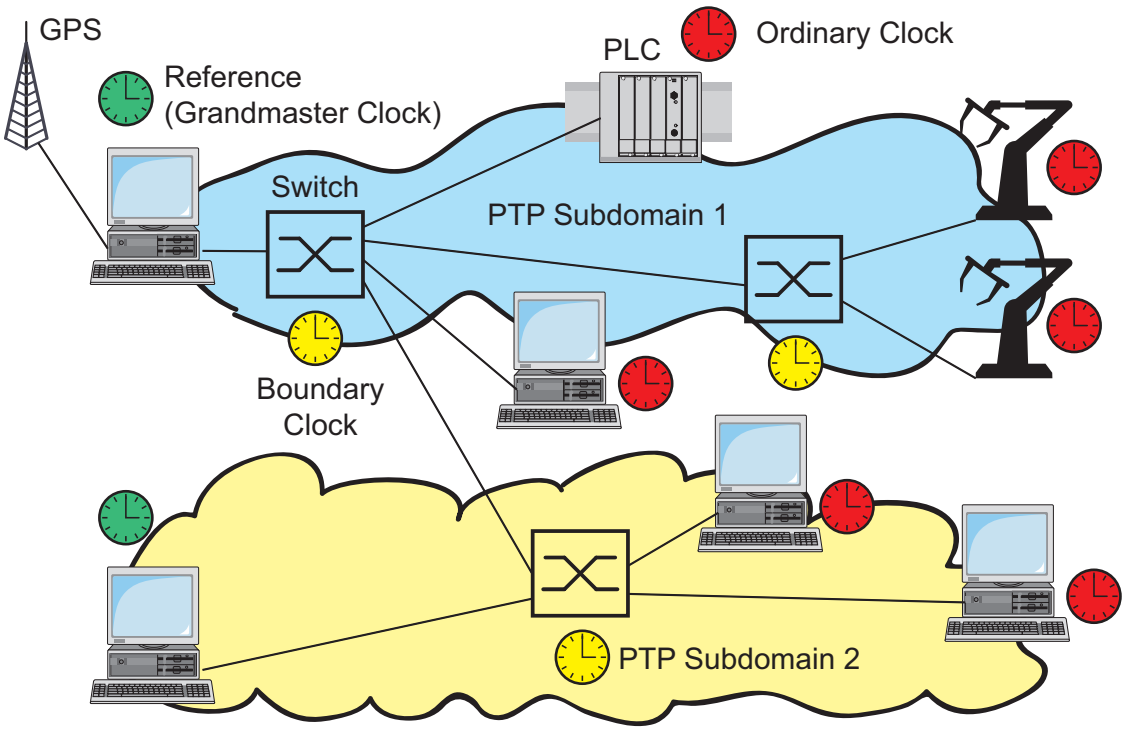


Figure 28: PTP Subdomains

8 Network Load Control

To optimize the data transmission, the device provides you with the following functions for controlling the network load:

- Settings for direct packet distribution (MAC address filter)
- Multicast settings
- Rate limiter
- Prioritization - QoS
- Flow control
- Virtual LANs (VLANs)

8.1 Direct Packet Distribution

With direct packet distribution, you help protect the device from unnecessary network loads. The device provides you with the following functions for direct packet distribution:

- Store-and-forward
- Multi-address capability
- Aging of learned addresses
- Static address entries
- Disabling the direct packet distribution

8.1.1 Store-and-forward

All data received by the device is stored, and its validity is checked. Invalid and defective data packets (> 1,502 bytes or CRC errors) as well as fragments (< 64 bytes) are rejected. Valid data packets are forwarded by the device.

8.1.2 Multi-Address Capability

The device learns all the source addresses for a port. Only packets with

- unknown destination addresses
- these destination addresses or
- a multi/broadcast destination address

in the destination address field are sent to this port. The device enters learned source addresses in its filter table (see on page 106 “Entering Static Addresses“).
The device can learn up to 8.000 addresses. This is necessary if more than one terminal device is connected to one or more ports. It is thus possible to connect several independent subnetworks to the device.

8.1.3 Aging of Learned Addresses

The device monitors the age of the learned addresses. Address entries which exceed a particular age - the aging time - are deleted by the device from its address table.
Data packets with an unknown destination address are flooded by the device.
Data packets with known destination addresses are selectively transmitted by the device.

Note: A reboot deletes the learned address entries.

- ☐ Select the `Switching:Global` dialog.
- ☐ Enter the aging time for all dynamic entries in the range from 10 to 630 seconds (unit: 1 second; default setting: 30).
  In connection with the router redundancy, select a time ≥ 30 seconds.

8.1.4 Entering Static Addresses

An important function of the device is the filter function. It selects data packets according to defined patterns, known as filters. These patterns are assigned distribution rules. This means that a data packet received by a device at a port is compared with the patterns. If there is a pattern that matches the data packet, a device then sends or blocks this data packet according to the distribution rules at the relevant ports.

The following are valid filter criteria:

- Destination address
- Broadcast address
- Multicast address
- VLAN membership

The individual filters are stored in the filter table (Forwarding Database, FDB). It consists of 3 parts: a static part and two dynamic parts.

- The management administrator describes the static part of the filter table (`dot1qStaticTable`).
- During operation, the device is capable of learning which of its ports receive data packets from which source address (see on page 104 “Multi-Address Capability“). This information is written to a dynamic part (`dot1qTpFdbTable`).
- Addresses learned dynamically from neighboring agents and those learned via GMRP are written to the other dynamic part.

Addresses already located in the static filter table are automatically transferred to the dynamic part by the device.
An address entered statically cannot be overwritten through learning.

Note: If the ring manager is active, it is not possible to make permanent unicast entries.

Note: This filter table allows you to create up to 100 filter entries for Multicast addresses.

☐ Select the `Switching:Filters for MAC Addresses` dialog.

Each row of the filter table represents one filter. Filters specify the way in which data packets are sent. They are set automatically by the Switch (learned status) or created manually. Data packets whose destination address is entered in the table are sent from the receiving port to the ports marked in the table. Data packets whose destination address is not in the table are sent from the receiving port to all other ports. In the "Create filter" dialog you can set up new filters. The following status settings are possible:

- `learned`: The filter was created automatically by the device.
- `invalid`: With this status you delete a manually created filter.
- `permanent`: The filter is stored permanently in the device or on the URL (see on page 57 “Saving settings“).
- `igmp`: The filter was created by IGMP Snooping.

To delete entries with the "learned" status from the filter table, select the `Basics:Restart` dialog and click "Reset MAC address table".

8.1.5 Disabling the Direct Packet Distribution

To enable you to observe the data at all the ports, the device allows you to disable the learning of addresses. When the learning of addresses is disabled, the device transfers all the data from all ports to all ports.

☐ Select the `Switching:Global` dialog.

UnCheck "Address Learning" to observe the data at all ports.

8.2 Multicast Application

8.2.1 Description of the Multicast Application

The data distribution in the LAN differentiates between 3 distribution classes on the basis of the addressed recipients:

- Unicast - one recipient
- Multicast - a group of recipients
- Broadcast - every recipient that can be reached

In the case of a Multicast address, the device forwards all data packets with a Multicast address to all ports. This leads to an increased bandwidth requirement.
Protocols such as GMRP and procedures such as IGMP Snooping enable the device to exchange information via the direct transmission of Multicast data packets. The bandwidth requirement can be reduced by distributing the Multicast data packets only to those ports to which recipients of these Multicast packets are connected.

You can recognize IGMP Multicast addresses by the range in which the address lies:

- MAC Multicast Address
  01:00:5E:00:00:00 - 01:00:5E:FF:FF:FF
  (in mask form 01:00:5E:00:00:00/24)
- Class D IP Multicast address
  224.0.0.0 - 239.255.255.255
  (in mask form 224.0.0.0/4)

8.2.2 Example of a Multicast Application

The cameras for monitoring machines normally transmit their images to monitors located in the machine room and to the control room.
In an IP transmission, a camera sends its image data with a Multicast address via the network.

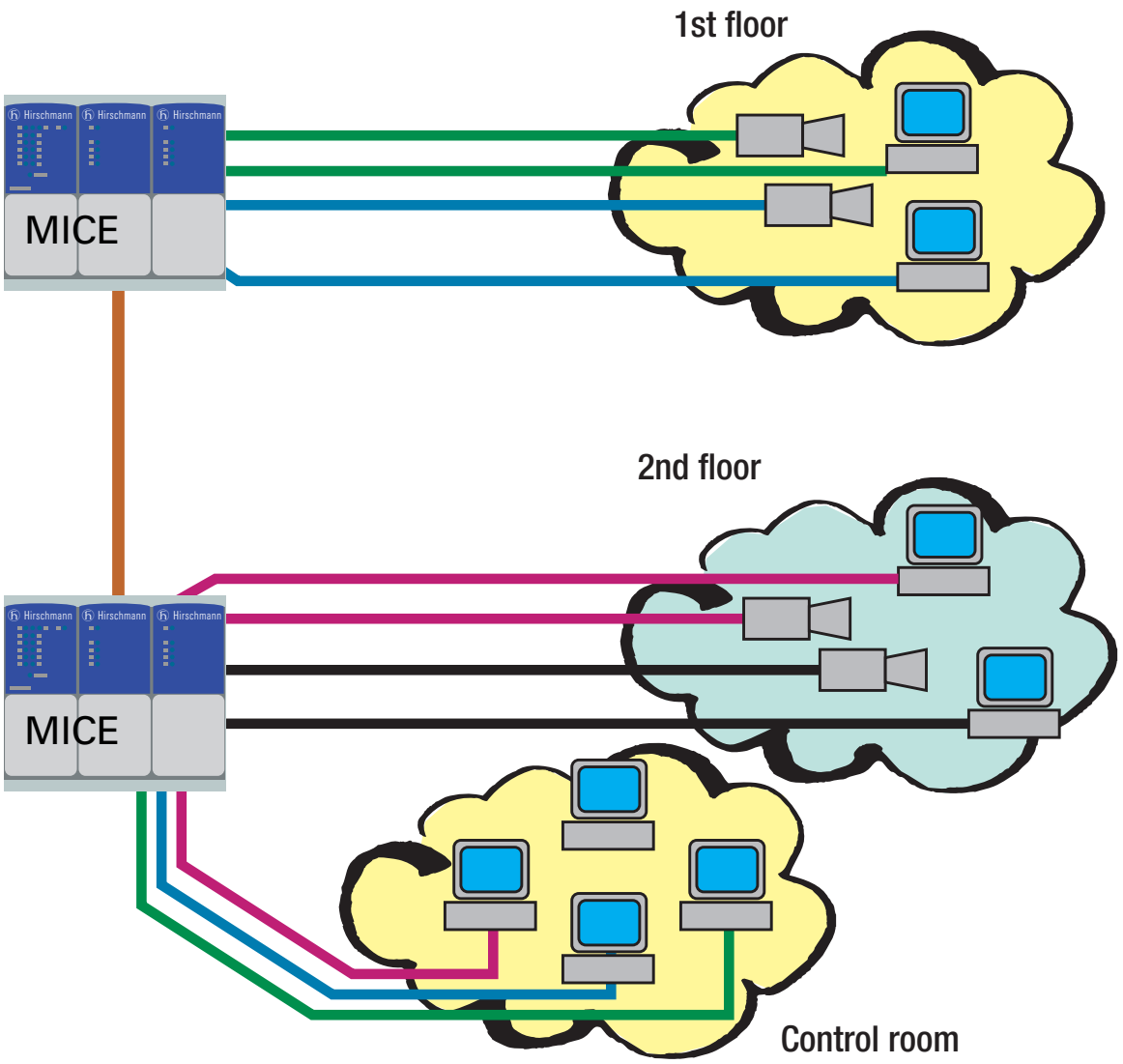


Figure 29: Example: Video surveillance in machine rooms

8.2.3 Description of IGMP Snooping

The Internet Group Management Protocol (IGMP) describes the distribution of Multicast information between routers and terminal devices on Layer 3.

Routers with an active IGMP function periodically send queries to find out which IP Multicast group members are connected to the LAN. Multicast group members reply with a Report message. This Report message contains all the parameters required by the IGMP. The router records the IP Multicast group address from the Report message in its routing table. The result of this is that it transfers frames with this IP Multicast group address in the destination field only in accordance with the routing table.

Devices which no longer want to be members of a Multicast group can cancel their membership by means of a Leave message (from IGMP version 2), and they do not transmit any more Report messages. In IGMP versions 1 and 2, the router removes the routing table entry if it does not receive any Report messages within a specified period of time (aging time).

If there are a number of routers with an active IGMP function in the network, then they work out among themselves (in IGMP version 2) which router carries out the Query function. If there is no router in the network, then a suitably equipped Switch can perform the Query function.

A Switch that connects a Multicast receiver with a router can evaluate the IGMP information with the aid of the IGMP Snooping procedure.

IGMP Snooping translates IP Multicast group addresses into MAC Multicast addresses, so that the IGMP functions can also be used by Layer 2 Switches. The Switch records the MAC addresses of the Multicast receivers, with are obtained via IGMP Snooping from the IP addresses, in the static address table. The Switch thus transmits these Multicast packets exclusively at the ports at which Multicast receivers are connected. The other ports are not affected by these packets.

A special feature of the device is that you can specify whether it should drop data packets with unregistered Multicast addresses, transmit them to all ports, or only to those ports at which the device received query packets. You also have the option of additionally sending known Multicast packets to query ports.

Default setting: “Off”.

8.2.4 Setting IGMP Snooping

☐ Select the `Switching:Multicast:IGMP` dialog.

Operation

The “Operation” frame allows you to enable/disable IGMP Snooping globally for the entire device.
If IGMP Snooping is disabled, then

- the device does not evaluate Query and Report packets received, and
- it sends (floods) received data packets with a Multicast address as the destination address to all ports.

Settings for IGMP Querier and IGMP

With these frames you can enter global settings for the IGMP settings and the IGMP Querier function.
Prerequisite: The IGMP Snooping function is activated globally.

IGMP Querier

“IGMP Querier active” allows you to enable/disable the Query function.

“Protocol version” allow you to select IGMP version 1, 2 or 3.

In “Send interval [s]” you specify the interval at which the device sends query packets (valid entries: 2-3,599 s, default setting: 125 s).

Note the connection between the parameters Max. Response Time, Send Interval and Group Membership Interval (see on page 113 “Parameter Values“).

IGMP-capable terminal devices respond to a query with a report message, thus generating a network load.
Select large sending intervals if you want to reduce the load on your network and can accept the resulting longer switching times.
Select small sending intervals if you require short switching times and can accept the resulting network load.

IGMP Settings

“Current querier IP address” shows you the IP address of the device that has the query function.

In “Max. Response Time” you specify the period within which the Multicast group members respond to a query (valid values: 1-3,598 s, default setting: 10 s).

Note the connection between the parameters Max. Response Time, Send Interval and Group Membership Interval (see on page 113 “Parameter Values“).

The Multicast group members select a random value within the maximum response time for their response, to prevent all the Multicast group members responding to the query at the same time.
Select a large value if you want to reduce the load on your network and can accept the resulting longer switching times.
Select a small value if you require short switching times and can accept the resulting network load.

In “Group Membership Interval” you specify the period for which a dynamic Multicast group remains entered in the device if it does not receive any report messages (valid values: 3-3,600 s, default setting: 260 s).

Note the connection between the parameters Max. Response Time, Send Interval and Group Membership Interval (see on page 113 “Parameter Values“).

Parameter Values

The parameters
– Max. Response Time,
– Send Interval and
– Group Membership Interval
have a relationship to each other:

Max. Response Time < Send Interval < Group Membership Interval.

If you enter values that contradict this relationship, the device then replaces these values with a default value or with the last valid values.

Parameter	Protocol Version	Value range	Default setting
Max. Response Time,	1, 2 3	1-25 seconds 1-3,598 seconds	10 seconds
Send Interval	1, 2, 3	2-3,599 seconds	125 seconds
Group Membership Interval	1, 2, 3	3-3,600 seconds	260 seconds

Table 7: Value range for
- Max. Response Time
- Send Interval
- Group Membership Interval

Multicasts

With these frames you can enter global settings for the Multicast functions.
Prerequisite: The IGMP Snooping function is activated globally.

Unknown Multicasts
In this frame you can determine how the device in IGMP mode sends packets with known and unknown MAC/IP Multicast addresses that were not learned through IGMP Snooping.

“Unknown Muilticasts” allows you to specify how the device transmits unknown Multicast packets:

- “Send to Query Ports”.
  The device sends the packets with an unknown MAC/IP Multicast address to all query ports.
- “Send to All Ports”.
  The device sends the packets with an unknown MAC/IP Multicast address to all ports.
- “Discard”.
  The device discards all packets with an unknown MAC/IP Multicast address.

Note: The way in which unlearned Multicast addresses are handled also applies to the reserved IP addresses from the “Local Network Control Block” (224.0.0.0 - 224.0.0.255). This can have an effect on higher-level routing protocols.

Known Multicasts
In this frame you can determine how the device in IGMP mode sends packets with known MAC/IP Multicast addresses that were learned through IGMP Snooping.

- “Send to query and registered ports”.
  The device sends the packets with a known MAC/IP Multicast address to all query ports and to registered ports.
  This standard setting sends all Multicasts to all query ports and to registered ports. The advantage of this is that it works in most applications without any additional configuration.
  Application: “Flood and Prune” routing in PIM-DM.
- “Send to registered ports”.
  The device sends the packets with a known MAC/IP Multicast address to registered ports.
  The advantage of this setting, which deviates from the standard, is that it uses the available bandwidth optimally through direct distribution. It requires additional port settings.
  Application: Routing protocol PIM-SM.

Settings per Port (Table)

- “IGMP on”
  This table column enables you to enable/disable the IGMP for each port when the global IGMP Snooping is enabled. Disabling the IGMP at a port prevents registration for this port.

- “IGMP Forward All”
  This table column enables you to enable/disable the “Forward All” IGMP Snooping function when the global IGMP Snooping is enabled. With the “Forward All” setting, the device sends to this port all data packets with a Multicast address in the destination address field.

  Note: If a number of routers are connected to a subnetwork, you must use IGMP version 1 so that all the routers receive all the IGMP reports.

  Note: If you use IGMP version 1 in a subnetwork, then you must also use IGMP version 1 in the entire network.

- “IGMP Automatic Query Port”
  This table column shows you which ports the device has learned as query ports, if “automatic” is selected in “Static Query Port”.

- “Static Query Port”
  The device sends IGMP report messages to the ports at which it receives IGMP queries (disable=default setting).
  This column allows you to also send IGMP report messages to: other selected ports (enable) or connected Hirschmann devices (automatic).

- “Learned Query Port”
  This table column shows you at which ports the device has received IGMP queries, if “disable” is selected in “Static Query Port”.

Note: If the device is connected to a HIPER ring, you can obtain quick reconfiguration of the network for data packets with registered Multicast destination addresses with the following settings:

- Switch on the IGMP Snooping on the ring ports and globally, and
- activate “IGMP Forward All” per port on the ring ports.

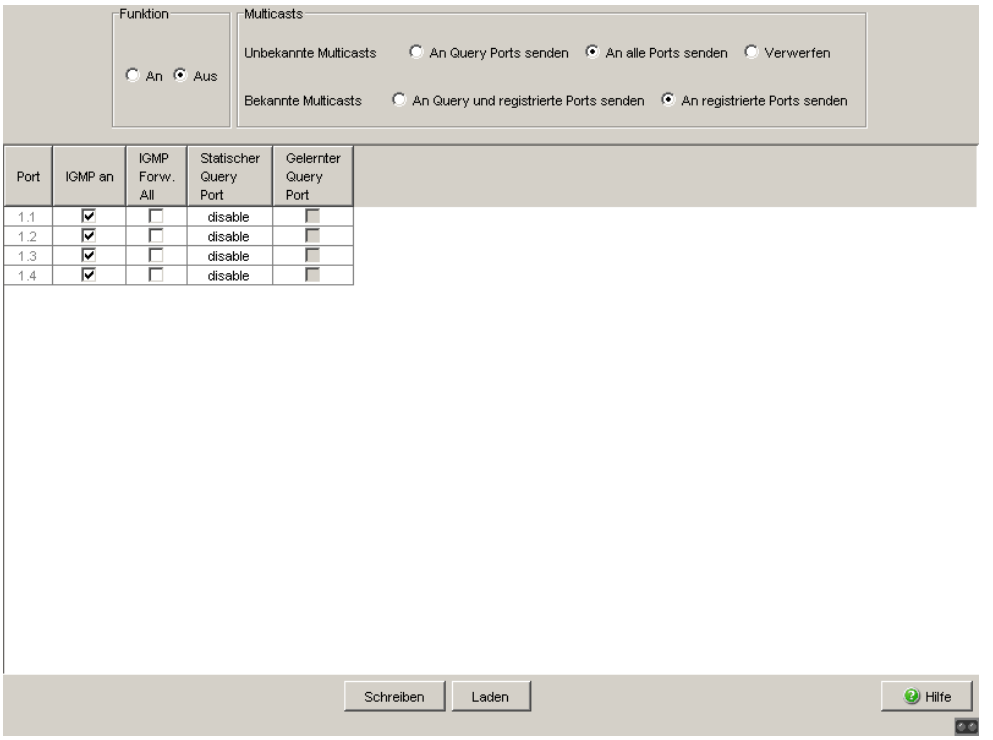


Figure 30: IGMP Snooping dialog

8.2.5 Setting GMRP

☐ Select the `Switching:Multicasts:GMRP` dialog.

Operation

Settings per Port (Table)

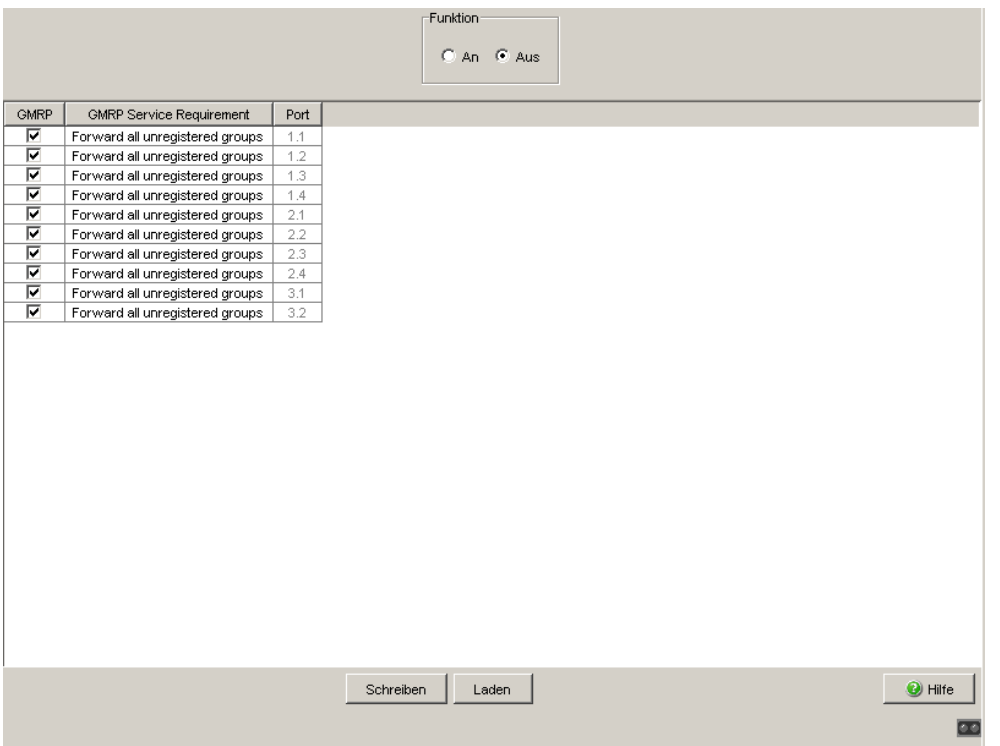


Figure 31: Multicasts dialog

8.3 Rate Limiter

8.3.1 Description of the Rate Limiter

The device can limit the rate of message traffic during periods of heavy traffic flow.

Entering a limit rate for each port specifies the amount of traffic the device is permitted to transmit and receive.

If the data load transmitted at this port exceeds the maximum load entered, the device will discard the excess data at this port.

A global setting enables/disables the rate limiter function at all ports.

Note: The limiter functions work exclusively on layer 2 and serve the purpose of limiting the effects of storms of those frame types (typically broadcasts) that the Switch floods. The limiter function ignores any protocol information of higher layers like IP or TCP. This may affect e.g., TCP traffic.

You can minimize this effects by:

- applying the limiter function only to particular frame types (e.g., to broadcasts, multicasts and unicasts with an unlearned destination address) and excluding unicasts with a learned destination address from the limitation,
- using the egress limiter function instead of the ingress limiter function because the former cooperates slightly better with TCP‘s flow control (reason: frames buffered by the internal switching buffer),
- increasing the aging time for learned unicast destination addresses.

8.3.2 Rate Limiter settings

☐ Select the `Switching:Rate Limiter` dialog.

- "Ingress Limiter (kbit/s)" allows you to enable or disable the input limiting function for all ports.
- "Egress Limiter (Pkt/s)" allows you to enable or disable the broadcast output limiter function at all ports.
- "Egress Limiter (kbit/s)" allows you to enable or disable the output limiter function for all packet types at all ports.

Setting options per port:

- "Ingress Packet Types" allows you to select the packet type for which the limit is to apply:
  - `All`, limits the total inbound data volume at this port.
  - `BC`, limits the broadcast packets received at this port.
  - `BC + MC`, limits broadcast packets and Multicast packets received at this port.
  - `BC + MC + uUC`, limits broadcast packets, Multicast packets, and unknown Unicast packets received at this port.
- Ingress Limiter Rate for the inbound packet type selected:
  - = 0, no ingress limit at this port.
  - > 0, maximum inbound traffic rate in kbit/s that can be received at this port.
- Egress Limiter Rate for broadcast packets:
  - = 0, no rate limit for outbound broadcast packets at this port.
  - > 0, maximum number of outbound broadcasts per second that can be sent at this port.
- Egress Limiter Rate for the entire data stream:
  - = 0, no rate limit for outbound data stream at this port.
  - > 0, maximum outbound transmission rate in kbit/s sent at this port.

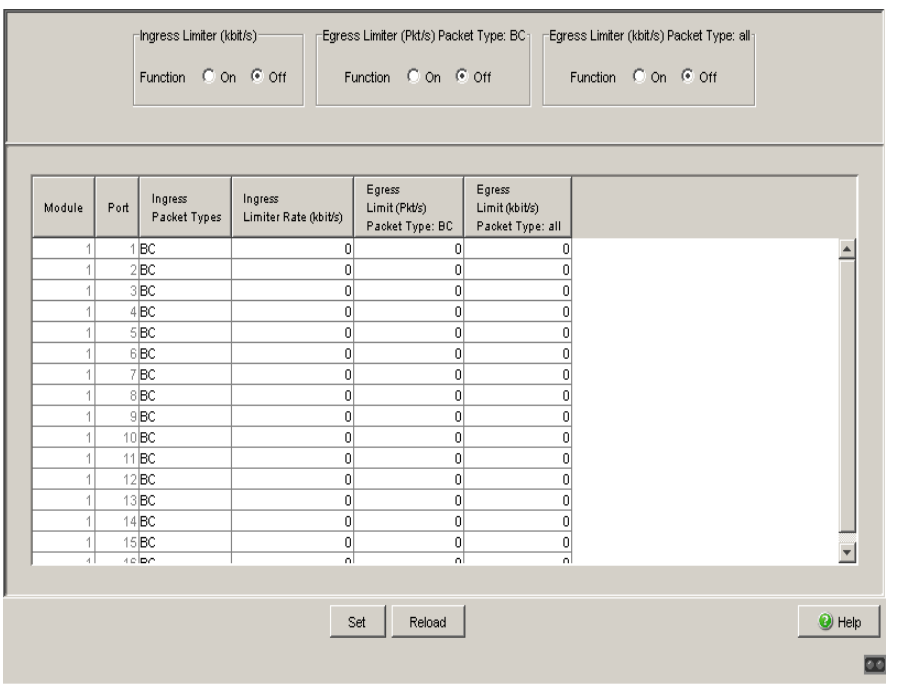


Figure 32: Rate Limiter

8.4 QoS/Priority

8.4.1 Description of Prioritization

This function prevents time-critical data traffic such as language/video or real-time data from being disrupted by less time-critical data traffic during periods of heavy traffic. By assigning high traffic classes for time-critical data and low traffic classes for less time-critical data, this provides optimal data flow for time-critical data traffic.

The device supports 4 priority queues (traffic classes in compliance with IEEE 802.1D). The assignment of received data packets to these classes is performed by

- the priority of the data packet contained in the VLAN tag when the receiving port was configured to “trust dot1p”.
- the QoS information (ToS/DiffServ) contained in the IP header when the receiving port was configured to “trust ip-dscp”.
- the port priority when the port was configured to “no trust”.
- the port priority when receiving non-IP packets when the port was configured to “trust ip-dscp”.
- the port priority when receiving data packets without a VLAN tag (see on page 71 “Configuring the Ports“) and when the port was configured to “trust dot1p”.
  Default setting: “trust dot1p”.

The device considers the classification mechanisms in the sequence shown above.

Data packets can contain prioritizing/QoS information:

- VLAN priority based on IEEE 802.1Q/ 802.1D (Layer 2)

8.4.2 VLAN tagging

The VLAN tag is integrated into the MAC data frame for the VLAN and Prioritization functions in accordance with the IEEE 802 1Q standard. The VLAN tag consists of 4 bytes. It is inserted between the source address field and the type field.

For data packets with a VLAN tag, the device evaluates
- the priority information and
- the VLAN information if VLANs have been set up.

Data packets with VLAN tags containing priority information but no VLAN information (VLAN ID = 0), are known as Priority Tagged Frames.

Priority entered	Traffic class (default setting)	IEEE 802.1D traffic type
0	1	Best effort (default)
1	0	Background
2	0	Standard
3	1	Excellent effort (business critical)
4	2	Controlled load (streaming multimedia)
5	2	Video, less than 100 milliseconds of latency and jitter
6	3	Voice, less than 10 milliseconds of latency and jitter
7	3	Network control reserved traffic

Table 8: Assignment of the priority entered in the tag to the traffic classes

Note: Network protocols and redundancy mechanisms use the highest traffic class 3. Therefore, select other traffic classes for application data.

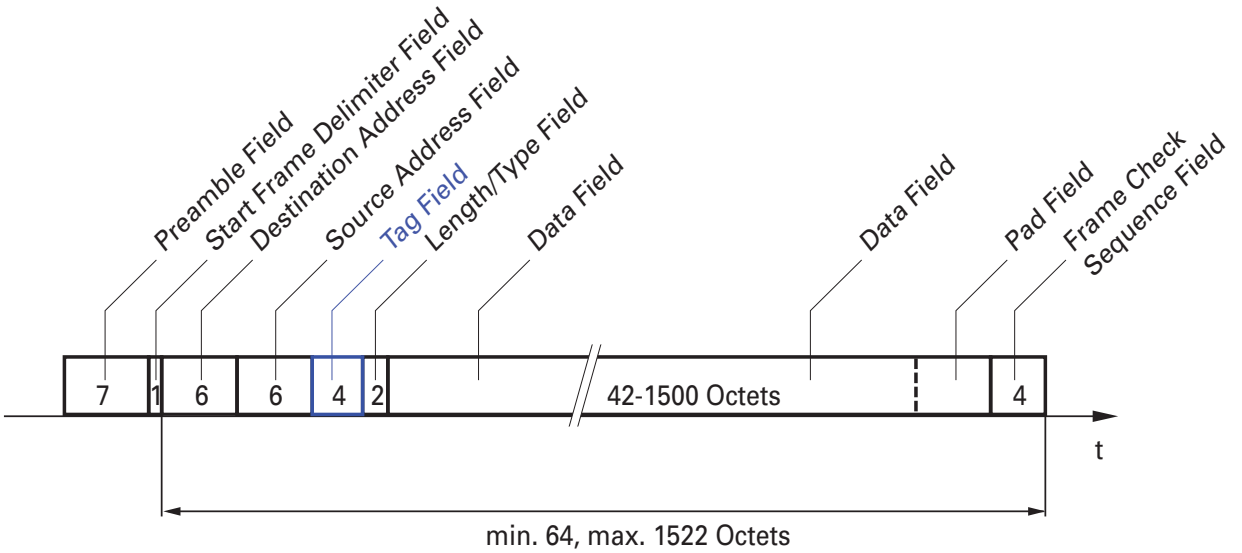


Figure 33: Ethernet data packet with tag

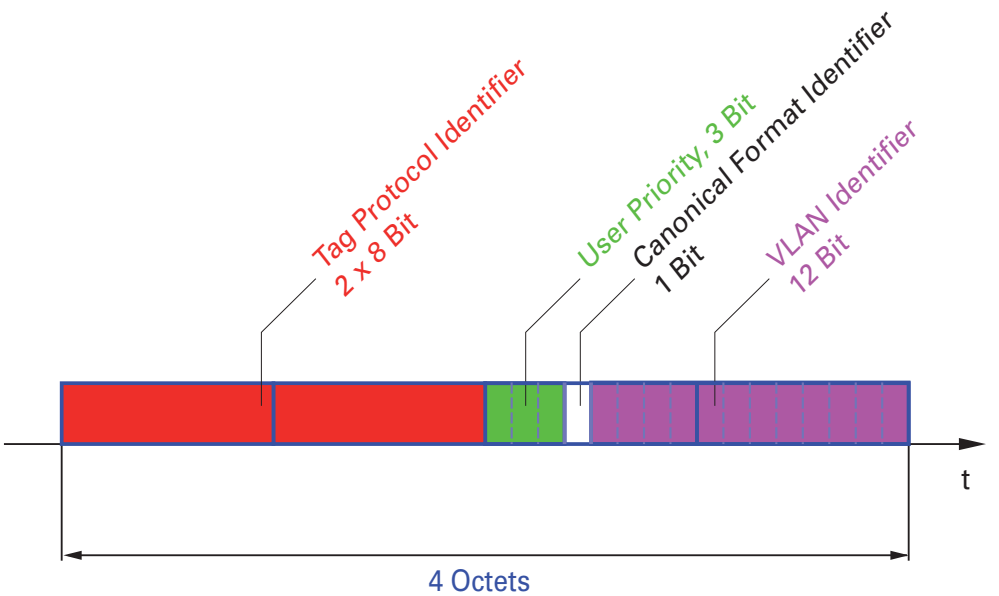


Figure 34: Tag format

When using VLAN prioritizing, note the following special features:

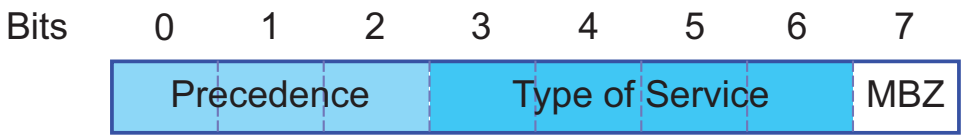
- End-to-end prioritizing requires the VLAN tags to be transmitted to the entire network, which means that all network components must be VLAN-capable.

- Routers cannot receive or send packets with VLAN tags via port-based router interfaces.

8.4.3 IP ToS / DiffServ

TYPE of Service

The Type of Service (ToS) field in the IP header (see table 9) has been part of the IP protocol from the start, and it is used to differentiate various services in IP networks. Even back then, there were ideas about differentiated treatment of IP packets, due to the limited bandwidth available and the unreliable connection paths. Because of the continuous increase in the available bandwidth, there was no need to use the ToS field. Only with the real-time requirements of today's networks has the ToS field become significant again. Selecting the ToS byte of the IP header enables you to differentiate between different services. However, this field is not widely used in practice.



Bits (0-2): IP Precedence Defined	Bits (3-6): Type of Service Defined	Bit (7)
111 - Network Control	0000 - [all normal]	0 - Must be zero
110 - Internetwork Control	1000 - [minimize delay]	
101 - CRITIC / ECP	0100 - [maximize throughput]	
100 - Flash Override	0010 - [maximize reliability]	
011 - Flash	0001 - [minimize monetary cost]	
010 - Immediate		
001 - Priority		
000 - Routine		

Table 9: ToS field in the IP header

Differentiated Services

The newly defined Differentiated Services field in the IP header (see fig. 35) - often known as the DiffServ code point or DSCP, replaces the ToS field and is used to mark the individual packets with a DSCP. Here the packets are divided into different quality classes. The first 3 bits of the DSCP are used to divide the packets into classes. The next 3 bits are used to further divide the classes on the basis of different criteria. In contrast to the ToS byte, DiffServ uses six bits for the division into classes. This results in up to 64 different service classes.

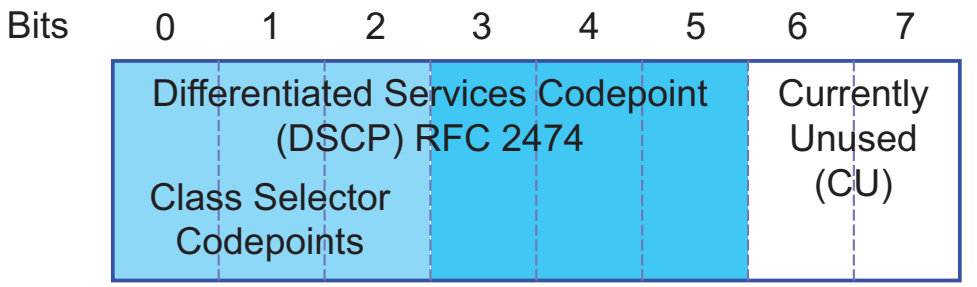


Figure 35: Differentiated Services field in the IP header

The different DSCP values get the device to employ a different forwarding behavior, namely Per-Hop Behavior (PHB). PHB classes:

- Class Selector (CS0-CS7): For reasons of compatibility to TOS/IP Precedence
- Expedited Forwarding (EF): Premium service.
  Reduced delay, jitter + packet loss (RFC2598)
- Assured Forwarding (AF): Provides a differentiated schema for handling different data traffic (RFC2597).
- Default Forwarding/Best Effort: No particular prioritizing.

The PHB class selector assigns the 7 possible IP precedence values from the old ToS field to specific DSCP values, thus ensuring the downwards compatibility.

ToS Meaning	Precedence Value	Assigned DSCP
Network Control	111	CS7 (111000)
Internetwork Control	110	CS6 (110000)
Critical	101	CS5 (101000)
Flash Override	100	CS4 (100000)
Flash	011	CS3 (011000)
Immediate	010	CS2 (010000)
Priority	001	CS1 (001000)
Routine	000	CS0 (000000)

Table 10: Assigning the IP precedence values to the DSCP value

DSCP value	DSCP name	Traffic class (default setting)
0	Best Effort /CS0	1
1-7		1
8	CS1	0
9,11,13,15		0
10,12,14	AF11,AF12,AF13	0
16	CS2	0
17,19,21,23		0
18,20,22	AF21,AF22,AF23	0
24	CS3	1
25,27,29,31		1
26,28,30	AF31,AF32,AF33	1
32	CS4	2
33,35,37,39		2
34,36,38	AF41,AF42,AF43	2
40	CS5	2
41,42,43,44,45,47		2
46	EF	2
48	CS6	3
49-55		3
56	CS7	3
57-63		3

Table 11: Mapping the DSCP values onto the traffic classes

8.4.4 Handling of Received Priority Information

The device provides 3 options, which can be chosen globally for all ports, for selecting how it handles received data packets that contain priority information.

- trust dot1p
  The device assigns VLAN-tagged packets to the different traffic classes according to their VLAN priorities. The assignment is based on the pre-defined table (see on page 122 “VLAN tagging“). You can modify this assignment. The device assigns the port priority to packets that it receives without a tag.
- untrusted
  The device ignores the priority information in the packet and always assigns the packets the port priority of the receiving port.
- trust ip-dscp
  The device assigns the IP packets to the different traffic classes according to the DSCP value in the IP header, even if the packet was also VLAN-tagged. The assignment is based on the pre-defined values (see table 11). You can modify this assignment.
  The device prioritizes non-IP packets according to the port priority.

8.4.5 Handling of Traffic Classes

For the handling of traffic classes, the device provides:

- Strict Priority

Description of Strict Priority

With the Strict Priority setting, the device first transmits all data packets that have a higher traffic class before transmitting a data packet with the next highest traffic class. The device transmits a data packet with the lowest traffic class only when there are no other data packets remaining in the queue. In some cases, a high level of data traffic can prevent packets with lower traffic classes from being sent.
In applications that are time- or latency-critical, such as VoIP or video, this method ensures that high-priority data is sent immediately..

8.4.6 Setting prioritization

Assigning the Port Priority

☐ Select the `QoS/Priority:Port Configuration` dialog.
☐ In the “Port Priority” column, you can specify the priority (0-7) with which the device sends data packets which it receives without a VLAN tag at this port.

Note: If you have set up VLANs, pay attention to the “Transparent mode” (see `Switching:VLAN:Global`)

`enable`	Switch to the Privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`interface 1/1`	Switch to the Interface Configuration mode of interface 1/1.
`vlan priority 3`	Assign port priority 3 to interface 1/1.
`exit`	Switch to the Configuration mode.

Assigning the VLAN Priority to the Traffic Classes

☐ Select the `QOS/Priority:802.1D/p-Mapping` dialog.
☐ In the "Traffic Class" column, enter the desired values.

`enable`	Switch to the Privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`classofservice dot1p-mapping 0 2`	Assign traffic class 2 to VLAN priority 0.
`classofservice dot1p-mapping 1 2`	Also assign traffic class 2 to VLAN priority 1.
`exit`	Switch to the privileged EXEC mode.
`show classofservice dot1p-mapping`	Display the assignment.

```
 User Priority    Traffic Class
 -------------    -------------
       0                2
       1                2
       2                0
       3                1
       4                2
       5                2
       6                3
       7                3
```

Assigning the traffic class to a DSCP

☐ Select the `QOS/Priority:IP DSCP Mapping` dialog.
☐ In the "Traffic Class" column, enter the desired values.

`enable`	Switch to the Privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`classofservice ip-dscp-mapping cs1 1`	Assign traffic class 1 to DSCP CS1.

```
show classofservice ip-dscp-mapping

    IP DSCP        Traffic Class
 -------------     -------------
   0(be/cs0)            2
   1                    2
   .
   .
   8(cs1)               1
   .
```

Always assign the DSCP priority to received IP data packets globally

☐ Select the `QoS/Priority:Global` dialog.
☐ Select `trustIPDSCP` in the "Trust Mode" line.

`enable`	Switch to the Privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`classofservice trust ip-dscp`	Assign the "trust ip-dscp" mode globally.
`exit`	Switch to the Configuration mode.
`exit`	Switch to the privileged EXEC mode.
`show classofservice trust`	Display the trust mode.
`Class of Service Trust Mode: IP DSCP`	

Configuring Layer 2 management priority

☐ Configure the VLAN ports to which the device sends management packets as a member of the VLAN that sends data packets with a tag (see on page 136 “Examples of VLANs“).

☐ Select the `QoS/Priority:Global` dialog.
☐ In the line `VLAN priority for management packets` you enter the value of the VLAN priority.

`enable`	Switch to the Privileged EXEC mode.
`network priority dot1p-vlan 7`	Assign the value 7 to the management priority so that management packets with the highest priority are sent.

`exit`	Switch to the privileged EXEC mode.
`show network`	Displays the management VLAN priority.

```
System IP Address.............................. 10.0.1.116
Subnet Mask.................................... 255.255.255.0
Default Gateway................................ 10.0.1.200
Burned In MAC Address.......................... 00:80:63:51:7A:80
Network Configuration Protocol (BootP/DHCP).... None
DHCP Client ID (same as SNMP System Name)...... "PowerMICE-517A80"
Network Configuration Protocol HiDiscovery..... Read-Write
Management VLAN ID............................. 1
Management VLAN Priority....................... 7
Management IP-DSCP Value....................... 0(be/cs0)
Web Mode....................................... Enable
JavaScript Mode................................ Enable
```

Configuring Layer 3 management priority

- ☐ Select the `QoS/Priority:Global` dialog.
- ☐ In the line `IP-DSCP value for management packets` you enter the IP-DSCP value with which the device sends management packets.

`enable`	Switch to the Privileged EXEC mode.
`network priority ip-dscp cs7`	Assign the value cs7 to the management priority so that management packets with the highest priority are handled.
`exit`	Switch to the privileged EXEC mode.
`show network`	Displays the management VLAN priority.

```
System IP Address.............................. 10.0.1.116
Subnet Mask.................................... 255.255.255.0
Default Gateway................................ 10.0.1.200
Burned In MAC Address.......................... 00:80:63:51:7A:80
Network Configuration Protocol (BootP/DHCP).... None
DHCP Client ID (same as SNMP System Name)...... "PowerMICE-517A80"
Network Configuration Protocol HiDiscovery..... Read-Write
Management VLAN ID............................. 1
Management VLAN Priority....................... 7
Management IP-DSCP Value....................... 56(cs7)
Web Mode....................................... Enable
JavaScript Mode................................ Enable
```

8.5 Flow Control

8.5.1 Description of Flow Control

Flow control is a mechanism which acts as an overload protection for the device. During periods of heavy traffic, it holds off additional traffic from the network.

The example (see fig. 36) shows a graphic illustration of how the flow control works. Workstations 1, 2 and 3 want to simultaneously transmit a large amount of data to Workstation 4. The combined bandwidth of Workstations 1, 2 and 3 to the device is larger than the bandwidth of Workstation 4 to the device. This leads to an overflow of the send queue of port 4. The funnel on the left symbolizes this status.

If the flow control function at ports 1, 2 and 3 of the device is turned on, the device reacts before the funnel overflows. Ports 1, 2 and 3 send a message to the connected devices that no data can be received at present.

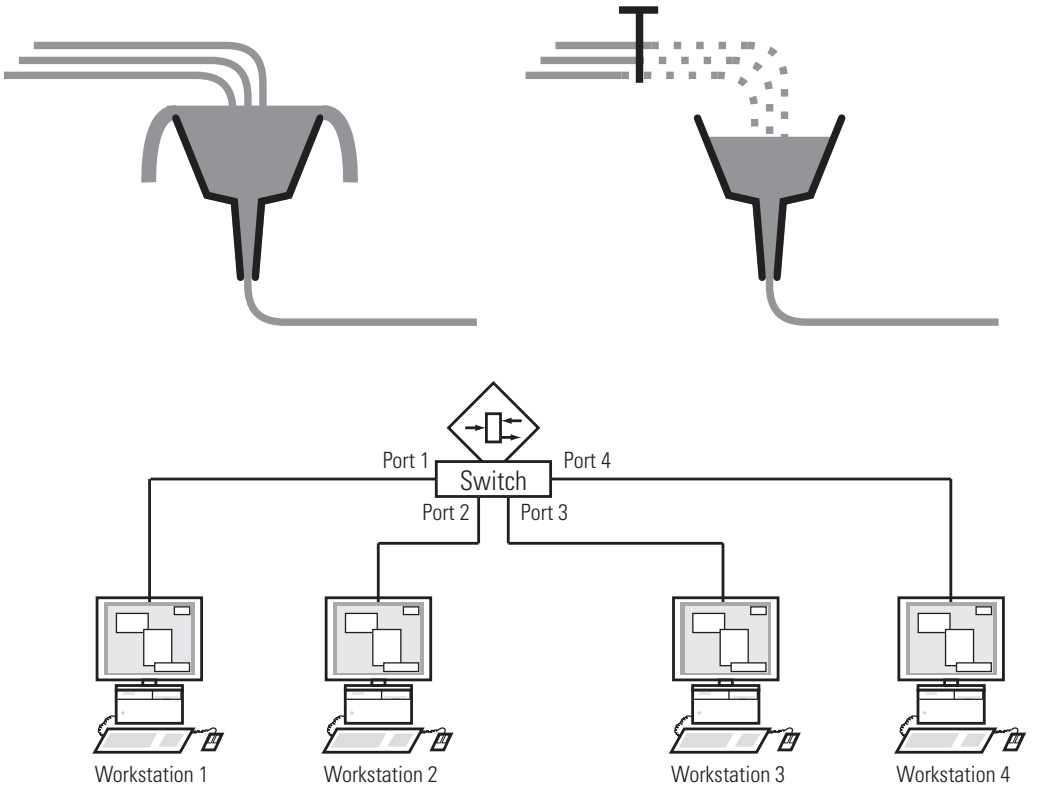


Figure 36: Example of flow control

Flow Control with a full duplex link

In the example (see fig. 36) there is a full duplex link between Workstation 2 and the device.
Before the send queue of port 2 overflows, the device sends a request to Workstation 2 to include a small break in the sending transmission.

Note: The devices RS20/30/40, MS20/30, Octopus, MACH 100, RSR and MACH 1000 support flow control in full duplex mode only.

Flow Control with a half duplex link

In the example (see fig. 36) there is a half duplex link between Workstation 2 and the device.
Before the send queue of port 2 overflows, the device sends data back so that Workstation 2 detects a collision and interrupts the sending process.

Note: The devices RS20/30/40, MS20/30, Octopus, MACH 100, RSR and MACH 1000 do not support flow control in half duplex mode.

8.5.2 Setting the Flow Control

☐ Select the `Basics:Port Configuration` dialog.
In the "Flow Control on" column, you checkmark this port to specify that flow control is active here. You also activate the global "Flow Control" switch in the `Switching:Global` dialog.

☐ Select the `Switching:Global` dialog.
With this dialog you can
- switch off the flow control at all ports or
- switch on the flow control at those ports for which the flow control is selected in the port configuration table.

Note: When you are using a redundancy function, you deactivate the flow control on the participating ports. Default setting: flow control deactivated globally and activated on all ports.
If the flow control and the redundancy function are active at the same time, there is a risk of the redundancy failing.

8.6 VLANs

8.6.1 VLAN Description

In the simplest case, a virtual LAN (VLAN) consists of a group of network participants in one network segment who can communicate with each other as if they belonged to a separate LAN.

More complex VLANs span out over multiple network segments and are also based on logical (instead of only physical) connections between network participants. Thus VLANs are an element of flexible network design, as you can reconfigure logical connections centrally more easily than cable connections.

The IEEE 802.1Q standard defines the VLAN function.

The most important benefits of VLANs are:

- Network load limiting
  VLANs can reduce the network load considerably as a Switch only transmits Broadcast/Multicast data packets and Unicast packets with unknown (unlearned) destination addresses within the virtual LAN. The rest of the data network is unaffected by this.

- Flexibility
  You have the option of forming user groups flexibly based on the function of the participants and not on their physical location or medium.

- Clarity
  VLANs give networks a clear structure and make maintenance easier.

8.6.2 Examples of VLANs

The following practical examples provide a quick introduction to the structure of a VLAN.

Example 1

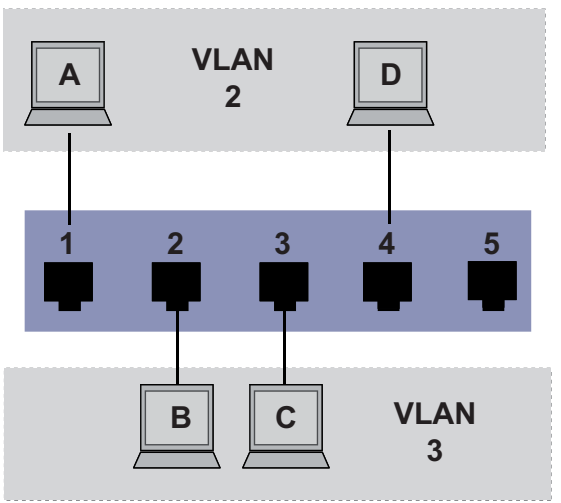


Figure 37: Example of a simple port-based VLAN

The example shows a minimal VLAN configuration (port-based VLAN). An administrator has connected multiple terminal devices to a transmission device and assigned them to 2 VLANs. This effectively prohibits any data transmission between the VLANs, whose members communicate only within their own VLANs.
When setting up the VLANs, you create communication rules for every port, which you enter in incoming (ingress) and outgoing (egress) tables. The ingress table specifies which VLAN ID a port assigns to the incoming data packets. Hereby, you use the port address of the terminal device to assign it to a VLAN.
The egress table specifies to which VLAN the frames sent from this port are assigned. Your entry also defines whether Ethernet frames sent from this port are to be tagged:

- T = with TAG field (T = tagged)
- U = without TAG field (U = untagged)

For the above example, the status of the TAG field of the data packets is not relevant, so you can generally set it to „U“.

Terminal	Port	Port VLAN identifier (PVID)
A	1	2
B	2	3
C	3	3
D	4	2
	5	1

Table 12: Ingress table

VLANID	Port				
	1	2	3	4	5
1					U
2	U			U	
3		U	U		

Table 13: Egress table

Proceed as follows to perform the example configuration:

☐ Configure VLAN

☐ Select the `Switching:VLAN:Static` dialog.

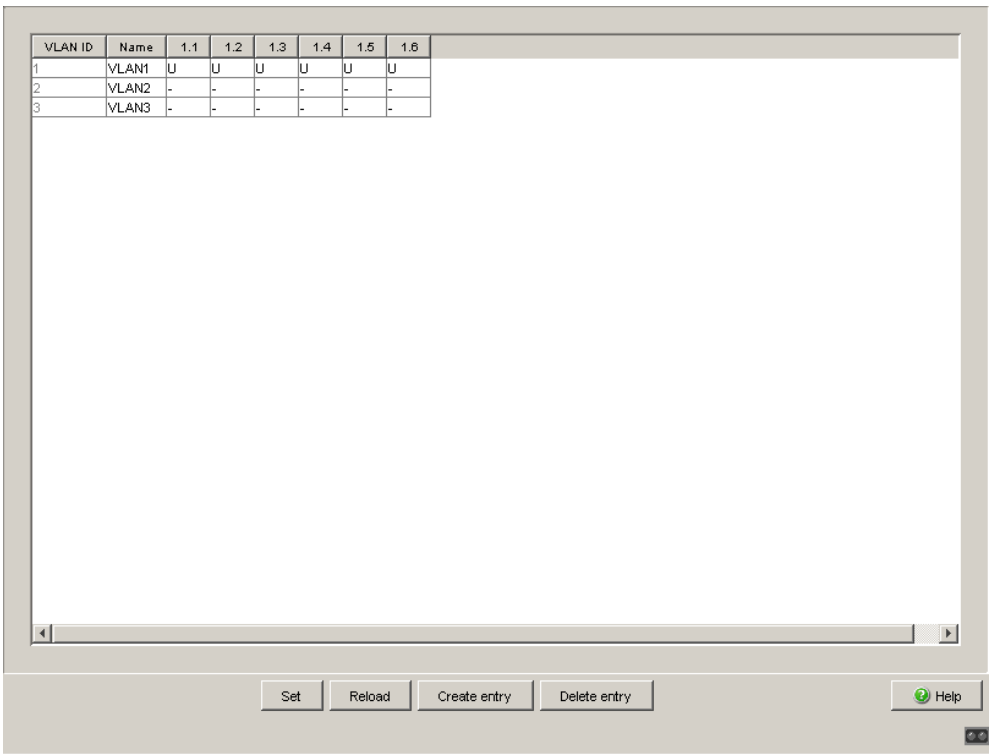


Figure 38: Creating and naming new VLANs

☐ Click on “Create Entry” to open a window for entering the VLAN ID.
☐ Assign VLAN ID 2 to the VLAN.
☐ Click on “OK”.
☐ You give this VLAN the name VLAN2 by clicking on the name field and entering the name. Also change the name for VLAN 1 from “Default” to “VLAN1”.
☐ Repeat the previous steps and create another VLAN with the VLAN ID 3 and the name VLAN3.

`enable`	Switch to the Privileged EXEC mode.
`vlan database`	Switch to the VLAN configuration mode.
`vlan 2`	Create a new VLAN with the VLAN ID 2.
`vlan name 2 VLAN2`	Give the VLAN with the VLAN ID 2 the name VLAN2.
`vlan 3`	Create a new VLAN with the VLAN ID 3.
`vlan name 3 VLAN3`	Give the VLAN with the VLAN ID 3 the name VLAN3.
`vlan name 1 VLAN1`	Give the VLAN with the VLAN ID 1 the name VLAN1.
`exit`	Leave the VLAN configuration mode.
`show vlan brief`	Display the current VLAN configuration.

```
Max. VLAN ID..................................... 4042
Max. supported VLANs.............................  255
Number of currently configured VLANs............    3
VLAN 0 Transparent Mode (Prio. Tagged Frames).. Disabled
VLAN ID VLAN Name                       VLAN Type VLAN Creation Time
---- -------------------------------- --------- -------------------
1       VLAN1                           Default    0 days, 00:00:05
2       VLAN2                           Static     0 days, 02:44:29
3       VLAN3                           Static     0 days, 02:52:26
```

☐ Configuring the ports

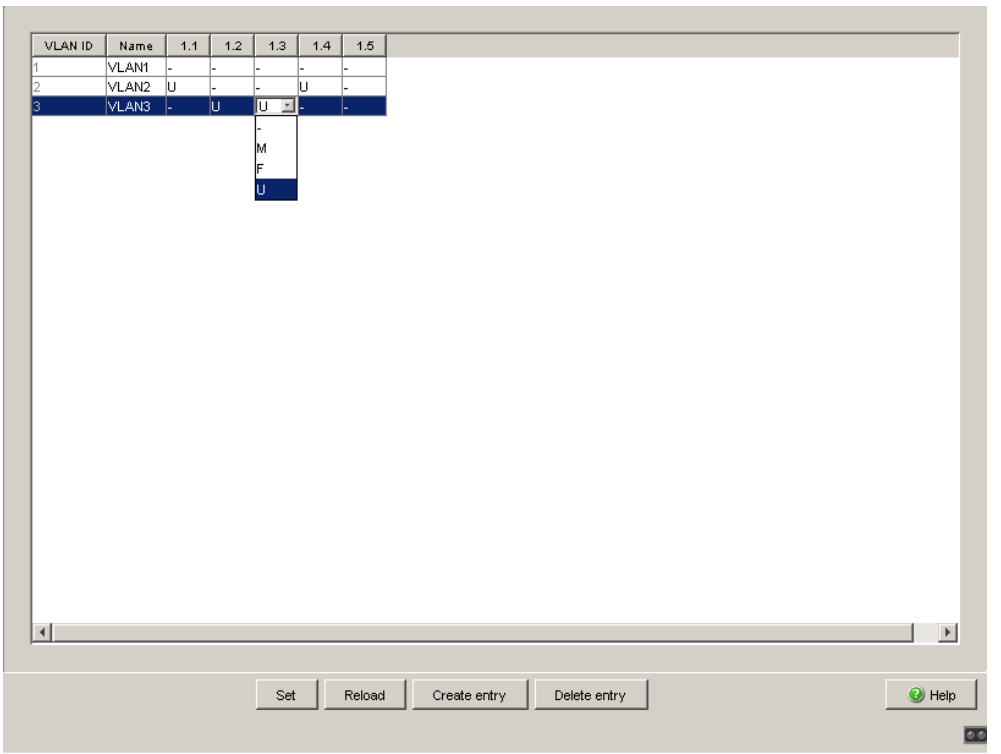


Figure 39: Defining the VLAN membership of the ports.

☐ Assign the ports of the device to the corresponding VLANs by clicking on the related table cell to open the selection menu and define the status. The selection options are:
- `-` = currently not a member of this VLAN (GVRP allowed)
- `T` = member of VLAN; send data packets with tag
- `U` = Member of the VLAN; send data packets without tag
- `F` = not a member of the VLAN (also disabled for GVRP)

Because terminal devices usually do not interpret data packets with a tag, you select the `U` setting here.

☐ Click “Set” to temporarily save the entry in the configuration.

☐ Select the `Switching:VLAN:Port` dialog.

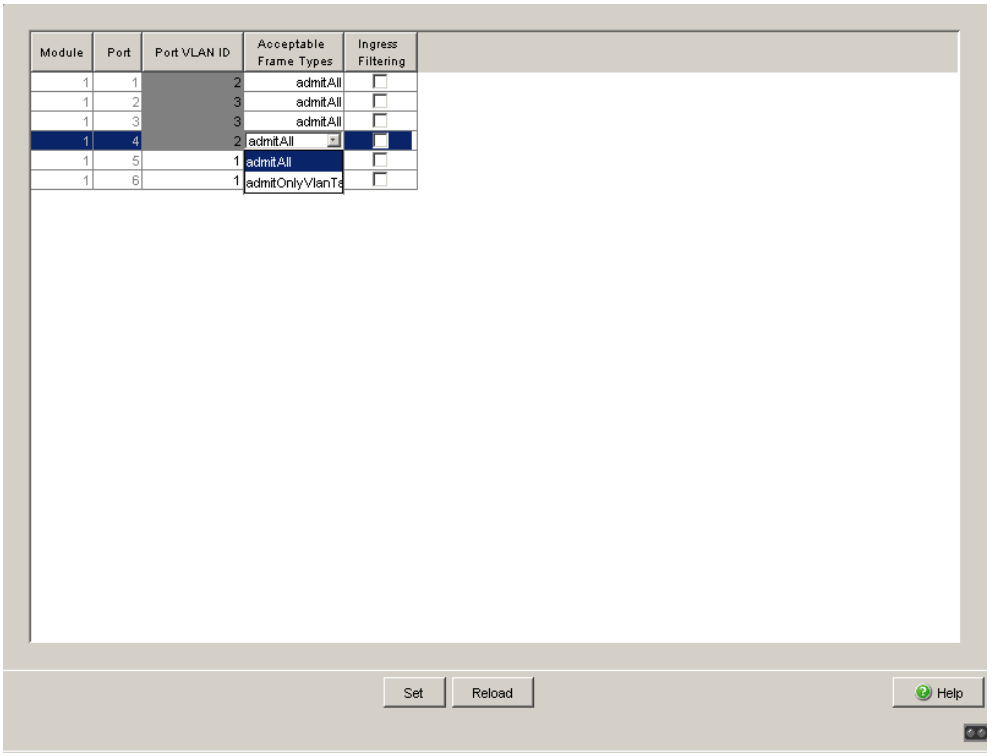


Figure 40: Assign and save Port VLAN ID, Acceptable Frame Types and Ingress Filtering

- ☐ Assign the Port VLAN ID of the related VLANs (2 or 3) to the individual ports - see table.
- ☐ Because terminal devices usually do not send data packets with a tag, you select the `admitAll` setting for “Acceptable Frame Types”.
- ☐ The setting for `Ingress Filter` does not affect how this example functions.
- ☐ Click “Set” to temporarily save the entry in the configuration.
- ☐ Select the `Basics: Load/Save` dialog.
- ☐ In the “Save” frame, select “To Device” for the location and click “Save” to permanently save the configuration in the active configuration.

`enable`	Switch to the Privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`interface 1/1`	Switch to the Interface Configuration mode of interface 1/1.
`vlan participation include 2`	Port 1/1 becomes member untagged in VLAN 2.
`vlan pvid 2`	Port 1/1 is assigned the port VLAN ID 2.
`exit`	Switch to the Configuration mode.
`interface 1/2`	Switch to the interface configuration mode for interface 1/2.
`vlan participation include 3`	Port 1/2 becomes member untagged in VLAN 3.
`vlan pvid 3`	Port 1/2 is assigned the port VLAN ID 3.
`exit`	Switch to the Configuration mode.
`interface 1/3`	Switch to the Interface Configuration mode of Interface 1/3.
`vlan participation include 3`	Port 1/3 becomes member untagged in VLAN 3.
`vlan pvid 3`	Port 1/3 is assigned the port VLAN ID 3.
`exit`	Switch to the Configuration mode.
`interface 1/4`	Switch to the interface configuration mode of interface 1/4.
`vlan participation include 2`	Port 1/4 becomes member untagged in VLAN 2.
`vlan pvid 2`	Port 1/4 is assigned the port VLAN ID 2.
`exit`	Switch to the Configuration mode.
`exit`	Switch to the privileged EXEC mode.
`show VLAN 3`	Show details for VLAN 3.

```
VLAN ID           : 3
VLAN Name         : VLAN3
VLAN Type         : Static
VLAN Creation Time: 0 days, 02:52:26 (System Uptime)
Interface   Current   Configured   Tagging
----------  --------  -----------  --------
1/1         Exclude   Autodetect   Tagged
1/2         Include   Include      Untagged
1/3         Include   Include      Untagged
1/4         Exclude   Autodetect   Tagged
1/5         Exclude   Autodetect   Tagged
```

Example 2

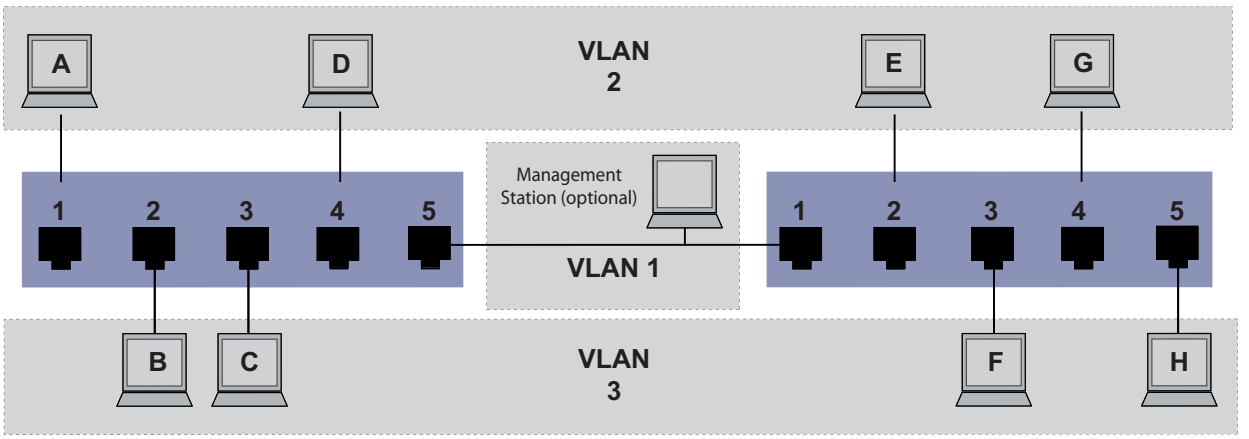


Figure 41: Example of a more complex VLAN constellation

The second example shows a more complex constellation with 3 VLANs (1 to 3). Along with the Switch from example 1, a second Switch (on the right in the example) is now used.
The terminal devices of the individual VLANs (A to H) are spread over two transmission devices (Switches). Such VLANs are therefore known as distributed VLANs. An optional Management Station is also shown, which enables access to all network components if it is configured correctly.

Note: In this case, VLAN 1 has no significance for the terminal device communication, but it is required to maintain the administration of the transmission devices via what is known as the Management VLAN.

As in the previous example, uniquely assign the ports with their connected terminal devices to a VLAN. With the direct connection between the two transmission devices (uplink), the ports transport packets for both VLANs. To differentiate these, “VLAN tagging” is used, which prepares the packets accordingly (see on page 122 “VLAN tagging“). This maintains the respective VLAN assignments.

Proceed as follows to perform the example configuration:
Add Uplink Port 5 to the ingress and egress tables from example 1.
Create new ingress and egress tables for the right switch, as described in the first example.
The egress table specifies to which VLAN the frames sent from this port are assigned. Your entry also defines whether Ethernet frames sent from this port are to be tagged:

- T = with TAG field (T = tagged)
- U = without TAG field (U = untagged)

In this example, tagged frames are used in the communication between the transmission devices (uplink), as frames for different VLANs are differentiated at these ports.

Terminal	Port	Port VLAN identifier (PVID)
A	1	2
B	2	3
C	3	3
D	4	2
Uplink	5	1

Table 14: Ingress table for device on left

Terminal	Port	Port VLAN identifier (PVID)
Uplink	1	1
E	2	2
F	3	3
G	4	2
H	5	3

Table 15: Ingress table for device on right

VLAN ID	Port				
	1	2	3	4	5
1					U
2	U			U	T
3		U	U		T

Table 16: Egress table for device on left

VLAN ID	Port				
	1	2	3	4	5
1	U				
2	T	U		U	
3	T		U		U

Table 17: Egress table for device on right

The communication relationships here are as follows: terminal devices at ports 1 and 4 of the left device and terminal devices at ports 2 and 4 of the right device are members of VLAN 2 and can thus communicate with each other. The behavior is the same for the terminal devices at ports 2 and 3 of the left device and the terminal devices at ports 3 and 5 of the right device. These belong to VLAN 3.
The terminal devices “see” their respective part of the network and cannot reach any other participant outside their VLAN. Broadcast and Multicast data packets, and Unicast packets with unknown (unlearned) target addresses as also only sent within a VLAN.

Here, VLAN tagging (IEEE 801.1Q) is used within the VLAN with the ID 1 (Uplink). You can see this from the letters (T) in the egress table of the ports.

The configuration of the example is the same for the device on the right. Proceed in the same way, using the ingress and egress tables created above to adapt the previously configured left device to the new environment.

Proceed as follows to perform the example configuration:

☐ Configure VLAN

☐ Select the `Switching:VLAN:Static` dialog.

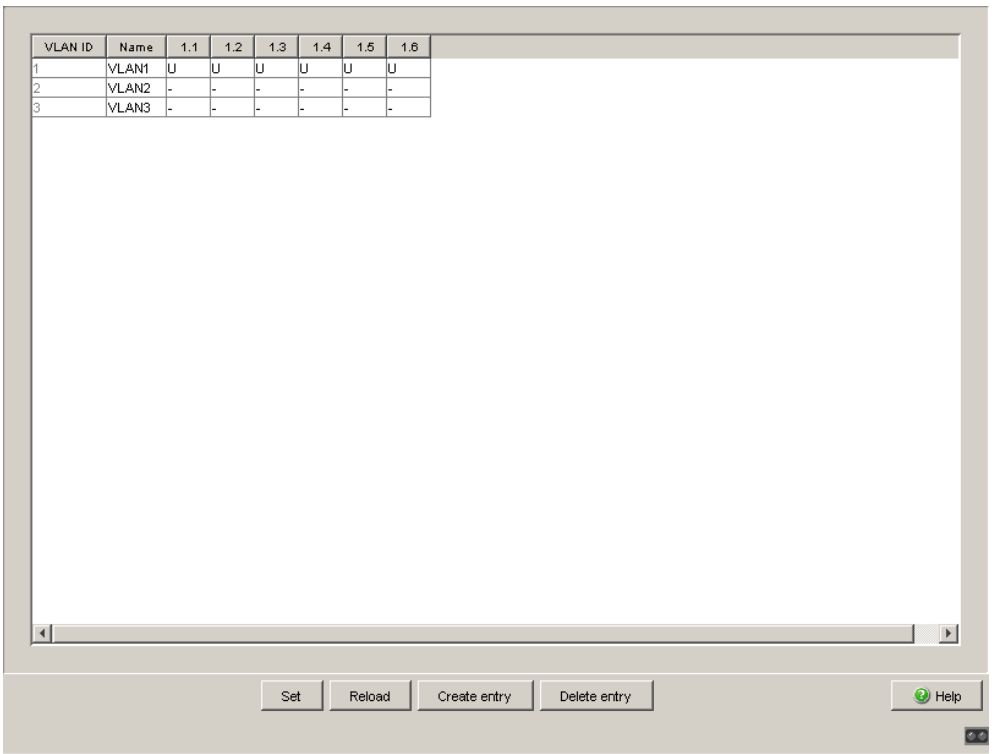


Figure 42: Creating and naming new VLANs

☐ Click on “Create Entry” to open a window for entering the VLAN ID.

☐ Assign VLAN ID 2 to the VLAN.

☐ You give this VLAN the name VLAN2 by clicking on the name field and entering the name. Also change the name for VLAN 1 from “Default” to “VLAN1”.

☐ Repeat the previous steps and create another VLAN with the VLAN ID 3 and the name “VLAN3”.

`enable`	Switch to the Privileged EXEC mode.
`vlan database`	Switch to the VLAN configuration mode.
`vlan 2`	Create a new VLAN with the VLAN ID 2.
`vlan name 2 VLAN2`	Give the VLAN with the VLAN ID 2 the name VLAN2.
`vlan 3`	Create a new VLAN with the VLAN ID 3.
`vlan name 3 VLAN3`	Give the VLAN with the VLAN ID 3 the name VLAN3.
`vlan name 1 VLAN1`	Give the VLAN with the VLAN ID 1 the name VLAN1.
`exit`	Switch to the privileged EXEC mode.
`show vlan brief`	Display the current VLAN configuration.

```
Max. VLAN ID..................................... 4042
Max. supported VLANs.............................  255
Number of currently configured VLANs...........    3
VLAN 0 Transparent Mode (Prio. Tagged Frames).. Disabled
VLAN ID VLAN Name                       VLAN Type VLAN Creation Time
---- -------------------------------- --------- -------------------
1       VLAN1                           Default    0 days, 00:00:05
2       VLAN2                           Static     0 days, 02:44:29
3       VLAN3                           Static     0 days, 02:52:26
```

☐ Configuring the ports

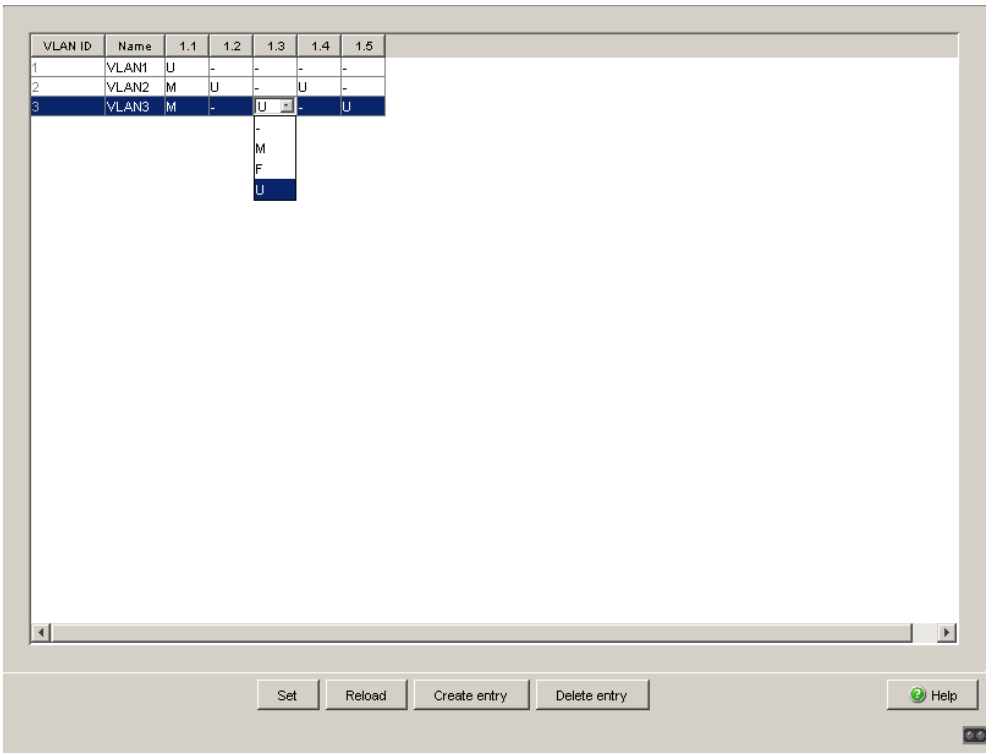


Figure 43: Defining the VLAN membership of the ports.

☐ Assign the ports of the device to the corresponding VLANs by clicking on the related table cell to open the selection menu and define the status. The selection options are:
- `-` = currently not a member of this VLAN (GVRP allowed)
- `T` = member of VLAN; send data packets with tag
- `U` = Member of the VLAN; send data packets without tag
- `F` = not a member of the VLAN (also disabled for GVRP)

Because terminal devices usually do not interpret data packets with a tag, you select the `U` setting. You only select the `T` setting at the uplink port at which the VLANs communicate with each other.

☐ Click “Set” to temporarily save the entry in the configuration.

☐ Select the `Switching:VLAN:Port` dialog.

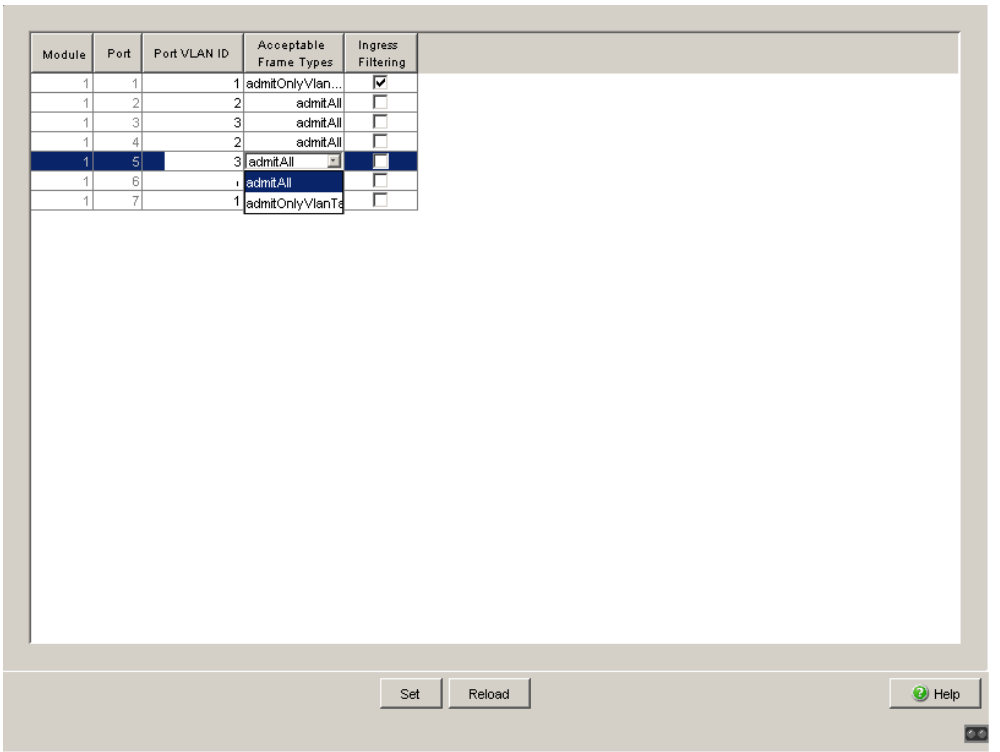


Figure 44: Assign and save Port VLAN ID, Acceptable Frame Types and Ingress Filtering

- ☐ Assign the ID of the related VLANs (1 to 3) to the individual ports.
- ☐ Because terminal devices usually do not send data packets with a tag, you select the `admitAll` setting for the terminal device ports. Configure the uplink port with `admit only VLAN tags`.
- ☐ Activate `Ingress Filtering` at the uplink port so that the VLAN tag is evaluated at this port.
- ☐ Click “Set” to temporarily save the entry in the configuration.
- ☐ Select the `Basics: Load/Save` dialog.
- ☐ In the “Save” frame, select “To Device” for the location and click “Save” to permanently save the configuration in the active configuration.

`enable`	Switch to the Privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`interface 1/1`	Switch to the Interface Configuration mode of interface 1/1.
`vlan participation include 1`	Port 1/1 becomes member untagged in VLAN 1.
`vlan participation include 2`	Port 1/1 becomes member untagged in VLAN 2.
`vlan tagging 2`	Port 1/1 becomes member tagged in VLAN 2.
`vlan participation include 3`	Port 1/1 becomes member untagged in VLAN 3.
`vlan tagging 3`	Port 1/1 becomes member tagged in VLAN 3.
`vlan pvid 1`	Port 1/1 is assigned the port VLAN ID 1.
`vlan ingressfilter`	Port 1/1 ingress filtering is activated.
`vlan acceptframe vlanonly`	Port 1/1 only forwards frames with a VLAN tag.
`exit`	Switch to the Configuration mode.
`interface 1/2`	Switch to the interface configuration mode for interface 1/2.
`vlan participation include 2`	Port 1/2 becomes member untagged in VLAN 2.
`vlan pvid 2`	Port 1/2 is assigned the port VLAN ID 2.
`exit`	Switch to the Configuration mode.
`interface 1/3`	Switch to the Interface Configuration mode of Interface 1/3.
`vlan participation include 3`	Port 1/3 becomes member untagged in VLAN 3.
`vlan pvid 3`	Port 1/3 is assigned the port VLAN ID 3.
`exit`	Switch to the Configuration mode.
`interface 1/4`	Switch to the interface configuration mode of interface 1/4.
`vlan participation include 2`	Port 1/4 becomes member untagged in VLAN 2.
`vlan pvid 2`	Port 1/4 is assigned the port VLAN ID 2.
`exit`	Switch to the Configuration mode.
`interface 1/5`	Switch to the interface configuration mode for port 1.5.
`vlan participation include 3`	Port 1/5 becomes member untagged in VLAN 3.
`vlan pvid 3`	Port 1/5 is assigned the port VLAN ID 3.
`exit`	Switch to the Configuration mode.
`exit`	Switch to the privileged EXEC mode.
`show vlan 3`	Show details for VLAN 3.

```
VLAN ID           : 3
VLAN Name         : VLAN3
VLAN Type         : Static
VLAN Creation Time: 0 days, 00:07:47 (System Uptime)
Interface   Current   Configured   Tagging
----------  --------  -----------  --------
1/1         Include   Include      Tagged
1/2         Exclude   Autodetect   Untagged
1/3         Include   Include      Untagged
1/4         Exclude   Autodetect   Untagged
1/5         Include   Include      Untagged
```

For further information on VLANs, see the reference manual and the integrated help function in the program.

9 Operation Diagnosis

The device provides you with the following diagnostic tools:

- Sending traps
- Monitoring the device status
- Out-of-band signaling via signal contact
- Port status indication
- Event counter at port level
- Detecting non-matching duplex modes
- SFP status display
- Topology Discovery
- Detecting IP address conflicts
- Detecting loops
- Reports
- Monitoring data traffic at a port (port mirroring)
- Syslog
- Event log

9.1 Sending Traps

If unusual events occur during normal operation of the device, they are reported immediately to the management station. This is done by means of what are called traps ? alarm messages ? that bypass the polling procedure ("Polling" means querying the data stations at regular intervals). Traps make it possible to react quickly to critical situations.

Examples of such events are:

- a hardware reset
- changes to the configuration
- segmentation of a port
- …

Traps can be sent to various hosts to increase the transmission reliability for the messages. A trap message consists of a packet that is not acknowledged.
The device sends traps to those hosts that are entered in the trap destination table. The trap destination table can be configured with the management station via SNMP.

9.1.1 List of SNMP Traps

All the possible traps that the device can send are listed in the following table.

Trap name	Meaning
authenticationFailure	is sent if a station attempts to access the agent without permission.
coldStart	is sent for both cold and warm starts during the boot process after successful management initialization.
hmAutoconfigAdapterTrap	is sent when AutoConfiguration AdapterACA is removed or plugged in.
linkDown	is sent if the link to a port is interrupted.
linkUp	is sent as soon as the link to a port is re-established.
hmTemperature	is sent if the temperature exceeds the set threshold values.
hmPowerSupply	is sent if the status of the voltage supply changes.
hmSigConRelayChange	is sent if the status of the signal contact changes during the operation monitoring.
newRoot	is sent if the sending agent becomes the new root of the spanning tree.
topologyChange	is sent if the transmission mode of a port changes.
risingAlarm	is sent if an RMON alarm input exceeds the upper threshold.
fallingAlarm	is sent if an RMON alarm input falls below the lower threshold.
hmPortSecurityTrap	is sent if a MAC/IP address is detected at the port which does not correspond to the current settings of: – hmPortSecPermission and – hmPorSecAction is set to either trapOnly (2) or portDisable (3).
hmModuleMapChange	is sent if the hardware configuration is changed.
hmBPDUGuardTrap	is sent if a BPDU is received at a port when the BPDU Guard function is active.
hmMrpReconfig	is sent if the configuration of the MRP-Ring changes.
hmRingRedReconfig	is sent if the configuration of the HIPER-Ring changes.
hmRingRedCplReconfig	is sent if the configuration of the redundant ring/network coupling changes.
hmSNTPTrap	is sent if errors occur in connection with the SNTP (e.g. server cannot be reached).
hmRelayDuplicateTrap	is sent if a duplicate IP address is detected in connection with DHCP Option 82.
lldpRemTablesChangeTrap	is sent if an entry in the topology remote table is changed.
hmConfigurationSavedTrap	is sent after the device has successfully saved its configuration locally.
hmConfigurationChangedTrap	is sent when you change the configuration of the device for the first time after it has been saved locally.

Table 18: Possible traps

Trap name	Meaning
hmAddressRelearnDetectTrap	is sent when Address Relearn Detection is activated and the threshold for the MAC addresses relearned at different ports has been exceeded. This process very probably indicates a loop situation in the network.
hmDuplexMismatchTrap	is sent if the device has detected a potential problem with the duplex mode of a port.

Table 18: Possible traps

9.1.2 SNMP Traps during Boot

The device sends the ColdStart trap every time it boots.

9.1.3 Configuring Traps

☐ Select the `Diagnostics:Alarms (Traps)` dialog.

This dialog allows you to determine which events trigger an alarm (trap) and where these alarms should be sent.

☐ Select “Create entry”.

☐ In the “IP Address” column, enter the IP address of the recipient to whom the traps should be sent.

☐ In the “Active” column, you select the entries which should be taken into account when traps are being sent.

☐ In the “Selection” frame, select the trap categories from which you want to send traps.

Note: You need read-write access for this dialog.

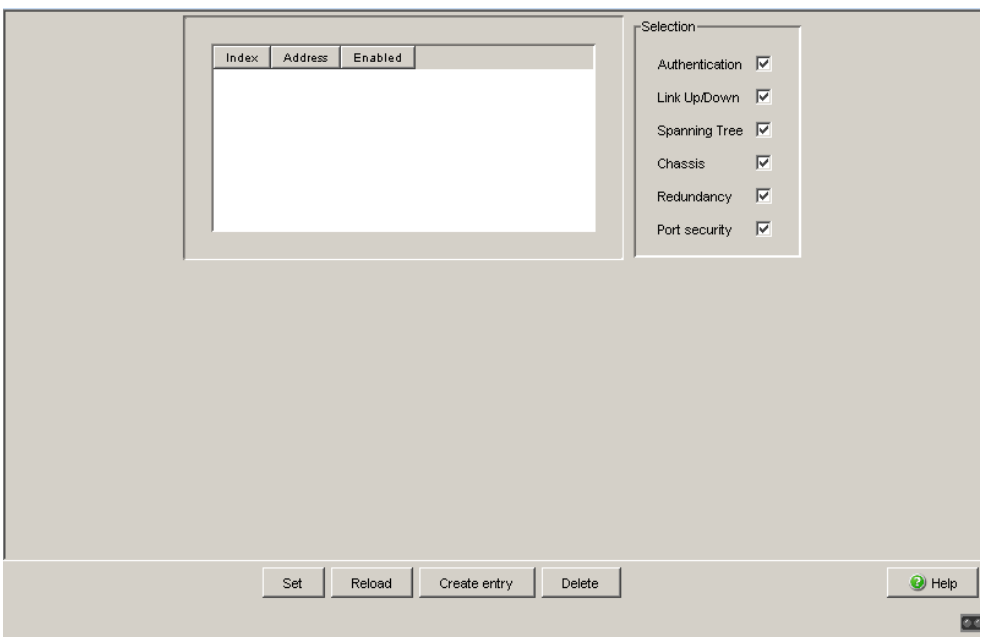


Figure 45: Alarms dialog

The events which can be selected are:

Name	Meaning
Authentication	The device has rejected an unauthorized access attempt (see the `Access for IP Addresses and Port Security` dialog).
Link Up/Down	At one port of the device, the link to another device has been established/ interrupted.
Spanning Tree	The topology of the Rapid Spanning Tree has changed.
Chassis	Summarizes the following events: – The status of a supply voltage has changed (see the System dialog). – The status of the signal contact has changed. To take this event into account, you activate “Create trap when status changes” in the `Diagnostics:Signal Contact 1/2` dialog. – A media module has been added or removed (only for modular devices). – The AutoConfiguration Adapter (ACA) was added or removed. – The configuration on the AutoConfiguration Adapter (ACA) does not match that of the device. – The temperature thresholds were not met or were exceeded. – The receiver power status of a port with an SFP module has changed (see dialog `Dialog:Ports:SFP Modules`). – The configuration has been successfully saved in the device and in the AutoConfiguration Adapter(ACA), if present. – The configuration has been changed for the first time after being saved in the device.
Redundancy	The redundancy status of the ring redundancy (redundant line active/ inactive) or (for devices that support redundant ring/network coupling) the redundant ring/network coupling (redundancy exists) has changed.
Port security	On one port a data packet has been received from an unauthorized terminal device (see the `Port Security` dialog).

Table 19: Trap categories

9.2 Monitoring the Device Status

The device status provides an overview of the overall condition of the device. Many process visualization systems record the device status for a device in order to present its condition in graphic form.
The device enables you to

- signal the device status out-of-band via a signal contact (see on page 163 “Monitoring the Device Status via the Signal Contact“)
- signal the device status by sending a trap when the device status changes
- detect the device status in the Web-based interface on the system side.
- query the device status in the Command Line Interface.

The device status of the device includes:

- Incorrect supply voltage,
  at least one of the two supply voltages is inoperative,
  the internal supply voltage is inoperative.
- The temperature threshold has been exceeded or has not been reached.
- The removal of a module (for modular devices).
- The removal of the ACA.
- The configuration on the ACA does not match that in the device.
- The interruption of the connection at at least one port. In the `Basic Settings:Port Configuration` menu, you define which ports the device signals if the connection is down (see on page 72 “Displaying connection error messages“). On delivery, there is no link monitoring.
- Event in the ring redundancy:
  Loss of the redundancy (in ring manager mode). On delivery, there is no ring redundancy monitoring.
- Event in the ring/network coupling:
  Loss of the redundancy. On delivery, there is no ring redundancy monitoring.
  The following conditions are also reported by the device in standby mode:
  – Defective link status of the control line
  – Partner device is in standby mode

Select the corresponding entries to decide which events the device status includes.

Note: With a non-redundant voltage supply, the device reports the absence of a supply voltage. If you do not want this message to be displayed, feed the supply voltage over both inputs or switch off the monitoring (see on page 163 “Monitoring the Device Status via the Signal Contact“).

9.2.1 Configuring the Device Status

- ☐ Select the `Diagnostics:Device Status` dialog.
- ☐ In the "Monitoring" field, you select the events you want to monitor.
- ☐ To monitor the temperature, you set the temperature thresholds in the `Basics:System` dialog at the end of the system data.

`enable`	Switch to the Privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`device-status monitor all error`	Include all the possible events in the device status determination.
`device-status trap enable`	Enable a trap to be sent if the device status changes.

Note: The above CLI commands activate the monitoring and the trapping respectively for all the supported components. If you want to activate or deactivate monitoring only for individual components, you will find the corresponding syntax in the CLI manual or in the help (Input ?) of the CLI console.

9.2.2 Displaying the Device Status

☐ Select the `Basics:System` dialog.

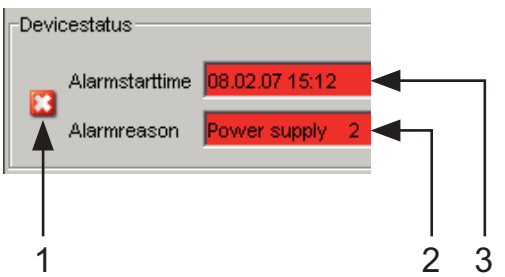


Figure 46: Device status and alarm display
1 - The symbol displays the device status
2 - Cause of the oldest existing alarm
3 - Start of the oldest existing alarm

`exit`	Switch to the privileged EXEC mode.
`show device-status`	Display the device status and the setting for the device status determination.

9.3 Out-of-band Signaling

The signal contact is used to control external devices and monitor the operation of the device. Function monitoring enables you to perform remote diagnostics.
The device reports the operating status via a break in the potential-free signal contact (relay contact, closed circuit):

- Incorrect supply voltage,
  at least one of the two supply voltages is inoperative,
  the internal supply voltage is inoperative.
- The temperature threshold has been exceeded or has not been reached.
- The removal of a module (for modular devices).
- The removal of the ACA.
- The configuration on the ACA does not match that in the device.
- The interruption of the connection at at least one port. In the `Basic Settings:Port Configuration` menu, you define which ports the device signals if the connection is down (see on page 72 “Displaying connection error messages“). On delivery, there is no link monitoring.
- Event in the ring redundancy:
  Loss of the redundancy (in ring manager mode). On delivery, there is no ring redundancy monitoring.
- Event in the ring/network coupling:
  Loss of the redundancy. On delivery, there is no ring redundancy monitoring.
  The following conditions are also reported by the device in standby mode:
  – Defective link status of the control line
  – Partner device is in standby mode

Select the corresponding entries to decide which events the device status includes.

Note: With a non-redundant voltage supply, the device reports the absence of a supply voltage. If you do not want this message to be displayed, feed the supply voltage over both inputs or switch off the monitoring (see on page 163 “Monitoring the Device Status via the Signal Contact“).

9.3.1 Controlling the Signal Contact

With this mode you can remotely control every signal contact individually.

Application options:

- Simulation of an error as an input for process control monitoring equipment.
- Remote control of a device via SNMP, such as switching on a camera.

☐ Select the `Diagnostics:Signal Contact 1/2)` dialog.

☐ In the "Mode Signal contact" frame, you select the "Manual setting" mode to switch the contact manually.

☐ Select "Opened" in the "Manual setting" frame to open the contact.

☐ Select "Closed" in the "Manual setting" frame to close the contact.

`enable`	Switch to the Privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`signal-contact 1 mode manual`	Select the manual setting mode for signal contact 1.
`signal-contact 1 state open`	Open signal contact 1.
`signal-contact 1 state closed`	Close signal contact 1.

9.3.2 Monitoring the Device Status via the Signal Contact

The "Device Status" option enables you, like in the operation monitoring, to monitor the device state (see on page 159 “Monitoring the Device Status“) via the signal contact.

9.3.3 Monitoring the Device Functions via the Signal Contact

Configuring the operation monitoring

- ☐ Select the `Diagnostics:Signal Contact` dialog.
- ☐ Select "Monitoring correct operation" in the "Mode signal contact" frame to use the contact for operation monitoring.
- ☐ In the "Monitoring correct operation" frame, you select the events you want to monitor.
- ☐ To monitor the temperature, you set the temperature thresholds in the `Basics:System` dialog at the end of the system data.

`enable`	Switch to the Privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`signal-contact 1 monitor all`	Includes all the possible events in the operation monitoring.
`signal-contact 1 trap enable`	Enables a trap to be sent if the status of the operation monitoring changes.

Displaying the signal contact's status

The device gives you 3 additional options for displaying the status of the signal contact:

- LED display on device,
- display in the Web-based interface,
- query in the Command Line Interface.

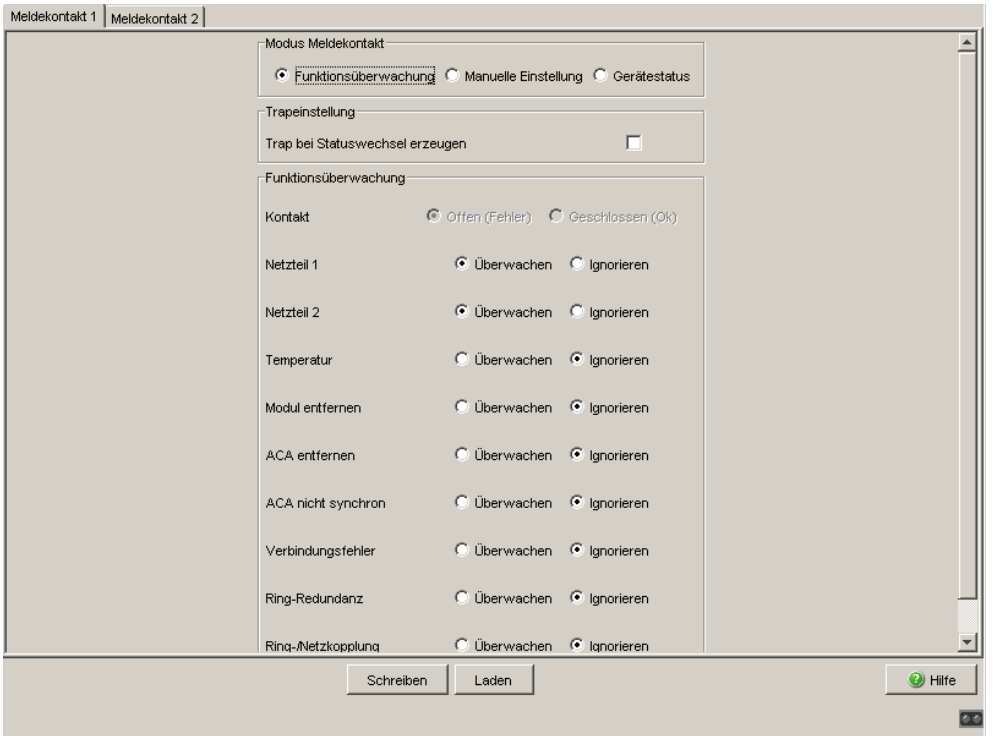


Figure 47: Signal Contact dialog

```
exit
show signal-contact 1
```

Switch to the privileged EXEC mode.

Displays the status of the operation monitoring and the setting for the status determination.

9.4 Port Status Indication

☐ Select the `Basics:System` dialog.
The device view shows the device with the current configuration. The symbols underneath the device view represent the status of the individual ports.

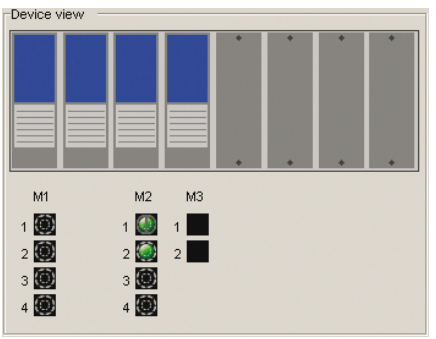


Figure 48: Device View

Meaning of the symbols:

The port (10, 100 Mbit/s, 1, 10 Gbit/s) is enabled and the connection is OK.

The port is disabled by the management and it has a connection.

The port is disabled by the management and it has no connection.

The port is in autonegotiation mode.

The port is in HDX mode.

The port is in RSTP discarding mode (100 Mbit/s).

The port is in routing mode (100 Mbit/s).

9.5 Event Counter at Port Level

The port statistics table enables experienced network administrators to identify possible detected problems in the network.
This table shows you the contents of various event counters. In the Restart menu item, you can reset all the event counters to zero using "Warm start", "Cold start" or "Reset port counter".
The packet counters add up the events sent and the events received.

Counter	Possible detected problem
Received fragments	– The controller of the connected device is inoperable – Electromagnetic interference in the transmission medium
CRC error	– The controller of the connected device is inoperable – Electromagnetic interference in the transmission medium – Defective component in the network
Collisions	– The controller of the connected device is inoperable – Network overextended/lines too long – Collision of a fault with a data packet

Table 20: Examples indicating possible detected problems

☐ Select the `Diagnostics:Ports:Statistics` dialog.

☐ To reset the counters, click on "Reset port counters" in the Basics:Restart dialog.

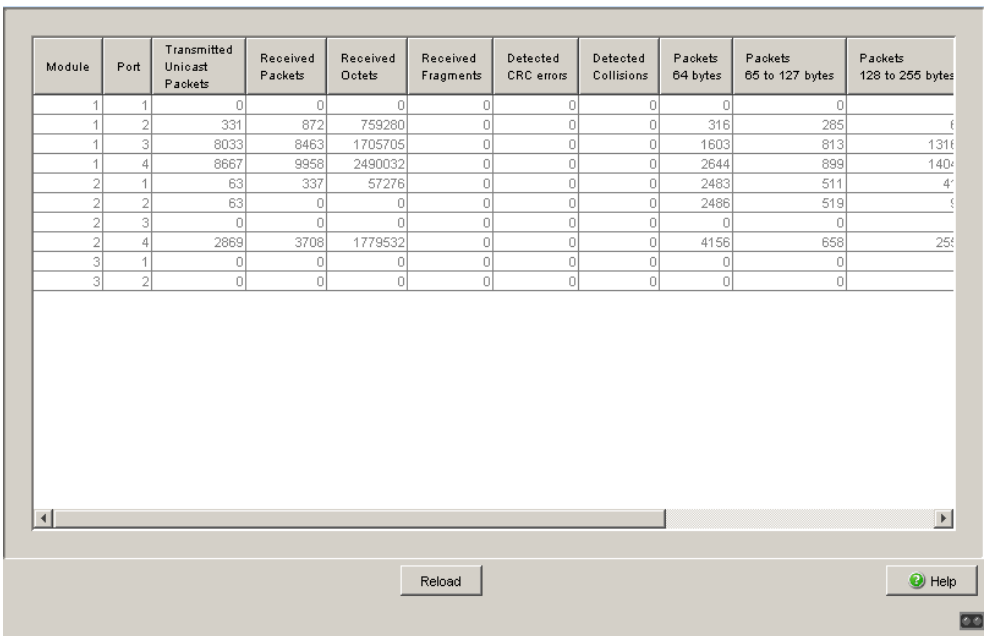


Figure 49: Port Statistics dialog

9.5.1 Detecting Non-matching Duplex Modes

If the duplex modes of 2 ports directly connected to each other do not match, this can cause problems that are difficult to track down. The automatic detection and reporting of this situation has the benefit of recognizing it before problems occur.

This situation can arise from an incorrect configuration, e.g. if you deactivate the automatic configuration at the remote port.

A typical effect of this non-matching is that at a low data rate, the connection seems to be functioning, but at a higher bi-directional traffic level the local device records a lot of CRC errors, and the connection falls significantly below its nominal capacity.

The device allows you to detect this situation and report it to the network management station. In the process, the device evaluates the error counters of the port in the context of the port settings.

Possible Causes of Port Error Events

The following table lists the duplex operating modes for TX ports together with the possible error events. The terms in the table mean:

- Collisions: In half-duplex mode, collisions mean normal operation.
- Duplex problem: Duplex modes do not match.
- EMI: Electromagnetic interference.
- Network extension: The network extension too great, or too many hubs are cascaded.

- Collisions, late collisions: In full-duplex mode, the port does not count collisions or late collisions.
- CRC error: The device only evaluates these errors as duplex problems in the manual full duplex mode.

No.	Autonegotiation	Current duplex mode	Detected error events (≥ 10)	Evaluation of duplex situation by device	Possible causes
1	On	Half duplex	None	OK	
2	On	Half duplex	Collisions	OK	
3	On	Half duplex	Late collisions	Duplex problem detected	Duplex problem, EMI, network extension
4	On	Half duplex	CRC error	OK	EMI
5	On	Full duplex	None	OK	
6	On	Full duplex	Collisions	OK	EMI
7	On	Full duplex	Late collisions	OK	EMI
8	On	Full duplex	CRC error	OK	EMI
9	Off	Half duplex	None	OK	
10	Off	Half duplex	Collisions	OK	
11	Off	Half duplex	Late collisions	Duplex problem detected	Duplex problem, EMI, network extension
12	Off	Half duplex	CRC error	OK	EMI
13	Off	Full duplex	None	OK	
14	Off	Full duplex	Collisions	OK	EMI
15	Off	Full duplex	Late collisions	OK	EMI
16	Off	Full duplex	CRC error	Duplex problem detected	Duplex problem, EMI

Table 21: Evaluation of non-matching of the duplex mode

Activating the detection

☐ Select the `Switching:Global` dialog.
☐ Select “Enable duplex mismatch detection”. The device then checks whether the duplex mode of a port might not match that of the remote port.
If the device detects a potential mismatch, it creates an entry in the event log and sends an alarm (trap).

`enable`	Switch to the Privileged EXEC mode.
`configure`	Switch to the Configuration mode.

`bridge duplex-mismatch-detect operation enable`	Activates the detection and reporting of non-matching duplex modes.
`bridge duplex-mismatch-detect operation disable`	Deactivates the detection and reporting of non-matching duplex modes.

9.6 Displaying the SFP Status

The SFP status display allows you to look at the current SFP module connections and their properties. The properties include:

- module type
- support provided in media module
- Temperature in ºC
- Tx Power in mW
- Receive power in mW

☐ Select the `Diagnostics:Ports:SFP Modules` dialog.

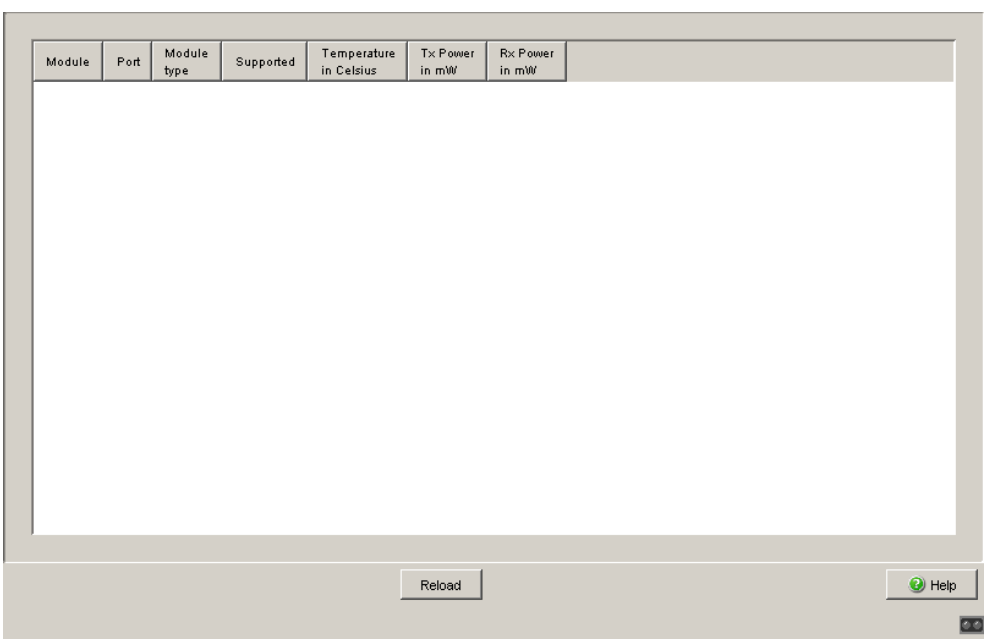


Figure 50: SFP Modules dialog

9.7 Topology Discovery

9.7.1 Description of Topology Discovery

IEEE 802.1AB describes the Link Layer Discovery Protocol (LLDP). LLDP enables the user to have automatic topology recognition for his LAN.

A device with active LLDP

- sends its own connection and management information to neighboring devices of the shared LAN. This can be evaluated there once these devices have also activated LLDP.
- receives connection and management information from neighboring devices of the shared LAN, once these devices have also activated LLDP.
- sets up a management information schema and object definition for saving information of neighboring devices with active LLDP.

A central element of the connection information is the exact, unique ID of a connection point: MSAP (MAC Service Access Point). This is made up of a device ID unique within the network and a port ID unique for this device. Content of the connection and management information:

- Chassis ID (its MAC address)
- Port ID (its port MAC address)
- Description of the port
- System Name
- System description
- Supported system capabilities
- Currently activated system capabilities
- Interface ID of the management address
- Port VLAN ID of the port
- Status of the autonegotiation at the port
- Medium, half and full duplex settings and speed setting of the port
- Information about whether a redundancy protocol is switched on at the port, and which one (for example, RSTP, HIPER-Ring, Fast-HIPER-Ring, MRP, Ring Coupling).

- Information about the VLANs which are set up in the switch (VLAN ID and VLAN name, regardless of whether the port is a VLAN member).

A network management station can call up this information from a device with LLDP activated. This information enables the network management station to map the topology of the network.

To exchange information, LLDP uses an IEEE MAC address which devices do not usually send. For this reason, devices without LLDP support discard LLDP packets. Thus a non-LLDP-capable device between 2 LLDP-capable devices prevents LLDP information exchange between these two devices. To get around this, Hirschmann devices send and receive additional LLDP packets with the Hirschmann Multicast MAC address 01:80:63:2F:FF:0B. Hirschmann devices with the LLDP function are thus also able to exchange LLDP information with each other via devices that are not LLDP-capable.

The Management Information Base (MIB) of an LLDP-capable Hirschmann device holds the LLDP information in the LLDP MIB and in the private hmLLDP.

9.7.2 Displaying the Topology Discovery Results

☐ Select the `Diagnostics:Topology Discovery` dialog.

This dialog allows you to switch on/off the topology discovery function (LLDP). The topology table shows you the collected information for neighboring devices. This information enables the network management station to map the structure of your network.

The option "Show LLDP entries exclusively" allows you to reduce the number of table entries. In this case, the topology table hides entries from devices without active LLDP support.

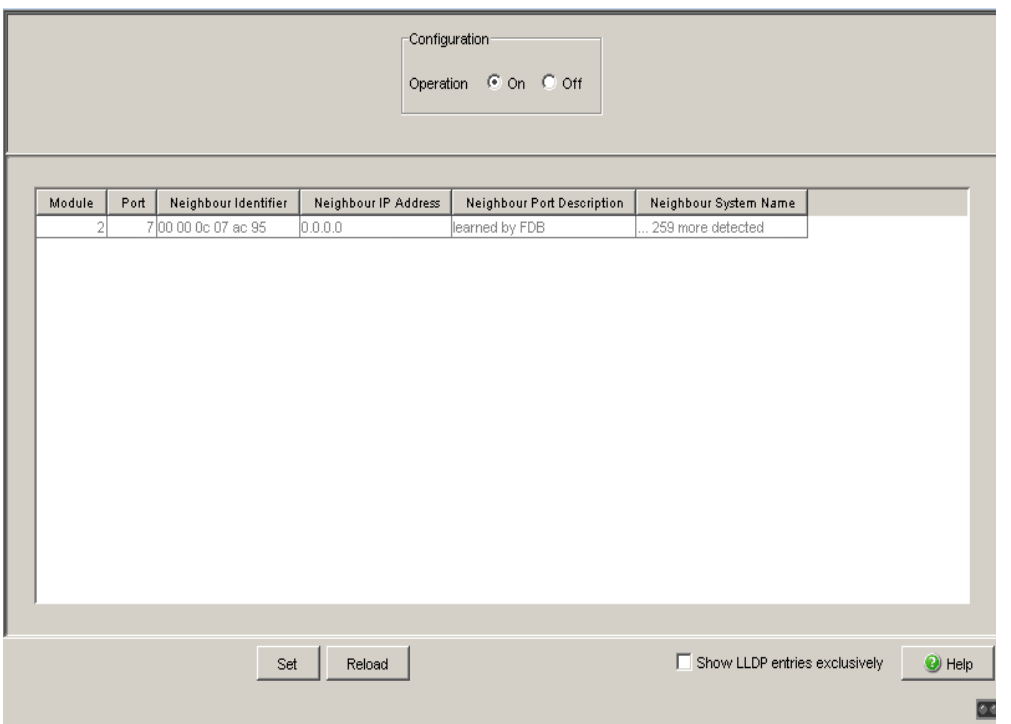


Figure 51: Topology discovery

If several devices are connected to one port, for example via a hub, the table will contain one line for each connected device.

If

- devices with active topology discovery function and
- devices without active topology discovery function

are connected to a port, the topology table hides the devices without active topology discovery.

If

- only devices without active topology discovery are connected to a port, the table will contain one line for this port to represent all devices. This line contains the number of connected devices. MAC addresses of devices that the topology table hides for the sake of clarity, are located in the address table (FDB), (see on page 106 “Entering Static Addresses“).

9.8 Detecting IP Address Conflicts

9.8.1 Description of IP Address Conflicts

By definition, each IP address may only be assigned once within a subnetwork. Should two or more devices erroneously share the same IP address within one subnetwork, this will inevitably lead to communication disruptions with devices that have this IP address. In his Internet draft, Stuart Cheshire describes a mechanism that industrial Ethernet devices can use to detect and eliminate address conflicts (Address Conflict Detection, ACD).

Mode	Meaning
enable	Enables active and passive detection.
disable	Disables the function
activeDetectionOnly	Enables active detection only. After connecting to a network or after an IP address has been configured, the device immediately checks whether its IP address already exists within the network. If the IP address already exists, the device will return to the previous configuration, if possible, and make another attempt after 15 seconds. This prevents the device from connecting to the network with a duplicate IP address.
passiveOnly	Enables passive detection only. The device listens passively on the network to determine whether its IP address already exists. If it detects a duplicate IP address, it will initially defend its address by employing the ACD mechanism and sending out gratuitous ARPs. If the remote device does not disconnect from the network, the management interface of the local device will then disconnect from the network. Every 15 seconds, it will poll the network to determine if there is still an address conflict. If there isn't, it will connect back to the network.

Table 22: Possible address conflict operation modes

9.8.2 Configuring ACD

☐ Select the Diagnostics:IP Address Conflict Detection dialog.
☐ With "Status" you enable/disable the IP address conflict detection or select the operating mode (see table 22).

9.8.3 Displaying ACD

☐ Select the `Diagnostics:IP Address Conflict Detection` dialog.

▶ In the table the device logs IP address conflicts with its IP address.
For each conflict the device logs:
- ▶ the time
- ▶ the conflicting IP address
- ▶ the MAC address of the device with which the IP address conflicted.

For each IP address, the device logs a line with the last conflict that occurred.

☐ You can delete this table by restarting the device.

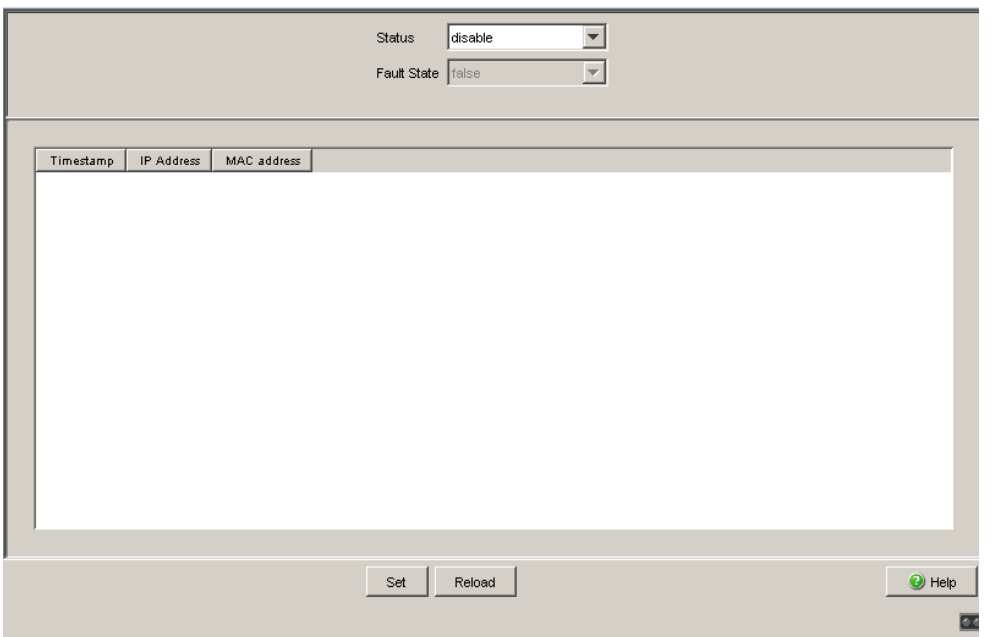


Figure 52: IP Address Conflict Detection dialog

9.9 Detecting Loops

Loops in the network, even temporary loops, can cause connection interruptions or data losses. The automatic detection and reporting of this situation allows you to detect it faster and diagnose it more easily.

An incorrect configuration can cause a loop, for example, if you deactivate Spanning Tree.

The device allows you to detect the effects typically caused by loops and report this situation automatically to the network management station. You have the option here to specify the magnitude of the loop effects that triggers the device to send a report.

A typical effect of a loop is that frames from multiple different MAC source addresses can be received at different ports of the device within a short time. The device evaluates how many of the same MAC source addresses it has learned at different ports within a time period.

Note: This procedure detects loops when the same MAC address is received at different ports. However, loops can also have other effects.
And it is also the case that the same MAC address being received at different ports can have other causes.

☐ Select the `Switching:Global` dialog.
☐ Select “Enable address relearn detection”. Enter the desired threshold value in the “Address relearn threshold” field.

If the address relearn detection is enabled, the device checks whether it has repeatedly learned the same MAC source addresses at different ports. This process very probably indicates a loop situation.
If the device detects that the threshold value set for the MAC addresses has been exceeded at its ports during the evaluation period (a few seconds), the device creates an entry in the log file and sends an alarm (trap). The preset threshold value is 1.

9.10 Reports

The following reports and buttons are available for the diagnostics:

- Log file.
  The log file is an HTML file in which the device writes all the important device-internal events.
- System information.
  The system information is an HTML file containing all system-relevant data.
- Download Switch-Dump.
  This button allows you to download system information as files in a ZIP archive.

In service situations, these reports provide the technician with the necessary information.

The following button is available as an alternative for operating the Web-based interface:

- Download JAR file.
  This button allows you to download the applet of the Web-based interface as a JAR file. Afterwards you have the option to start the applet outside a browser.
  This enables you to administer the device even when you have deactivated its Web server for security reasons.

☐ Select the `Diagnostics:Report` dialog.

☐ Click “Log File” to open the HTML file in a new browser window.

☐ Click “System Information” to open the HTML file in a new browser window.

☐ Click “Download Switch-Dump”.

☐ Select the directory in which you want to save the switch dump.

☐ Click “Save”.

The device creates the file name of the switch dumps automatically in the format <IP address>_<system name>.zip, e.g. for a device of the type PowerMICE: “10.0.1.112_PowerMICE-517A80.zip”.

☐ Click “Download JAR-File”.

☐ Select the directory in which you want to save the applet.

☐ Click “Save”.

The device creates the file name of the applet automatically in the format <device type><software variant><software version)>_<software revision of applet>.jar, e.g. for a device of type PowerMICE with software variant L3P: “pmL3P06000_00.jar”.

9.11 Monitoring Data Traffic at Ports (Port Mirroring)

The port mirroring function enables you to review the data traffic at up to 8 ports of the device for diagnostic purposes. The device additionally forwards (mirrors) the data for these ports to another port. This process is also called port mirroring.
The ports to be reviewed are known as source ports. The port to which the data to be reviewed is copied is called the destination port. You can only use physical ports as source or destination ports.

In port mirroring, the device copies valid incoming **and** outgoing data packets of the source port to the destination port. The device does not affect the data traffic at the source ports during port mirroring.
A management tool connected at the destination port, e.g. an RMON probe, can thus monitor the data traffic of the source ports in the sending and receiving directions.

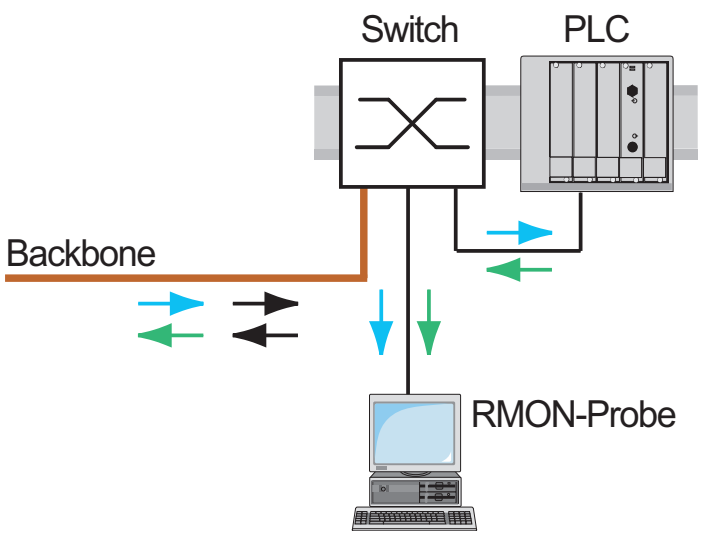


Figure 53: Port mirroring

☐ Select the `Diagnostics:Port Mirroring` dialog.

This dialog allows you to configure and activate the port mirroring function of the device.

☐ Select the source ports whose data traffic you want to review from the list of physical ports by checkmarking the relevant boxes.
You can select a maximum of 8 source ports. Ports that cannot be selected are displayed as inactive by the device, e.g. the port currently being used as the destination port, or if you have already selected 8 ports. Default setting: no source ports.

☐ Select the destination port to which you have connected your management tool from the list element in the “Destination Port” frame.
The device does not display ports that cannot be selected in the list, e.g. the ports currently being used as source ports. Default setting: port 0.0 (no destination port).

☐ Select “On” in the “Function” frame to switch on the function. Default setting: “Off”.

The “Reset configuration” button in the dialog allows you to reset all the port mirroring settings of the device to the state on delivery.

Note: When port mirroring is active, the specified destination port is used solely for reviewing, and does not participate in the normal data traffic.

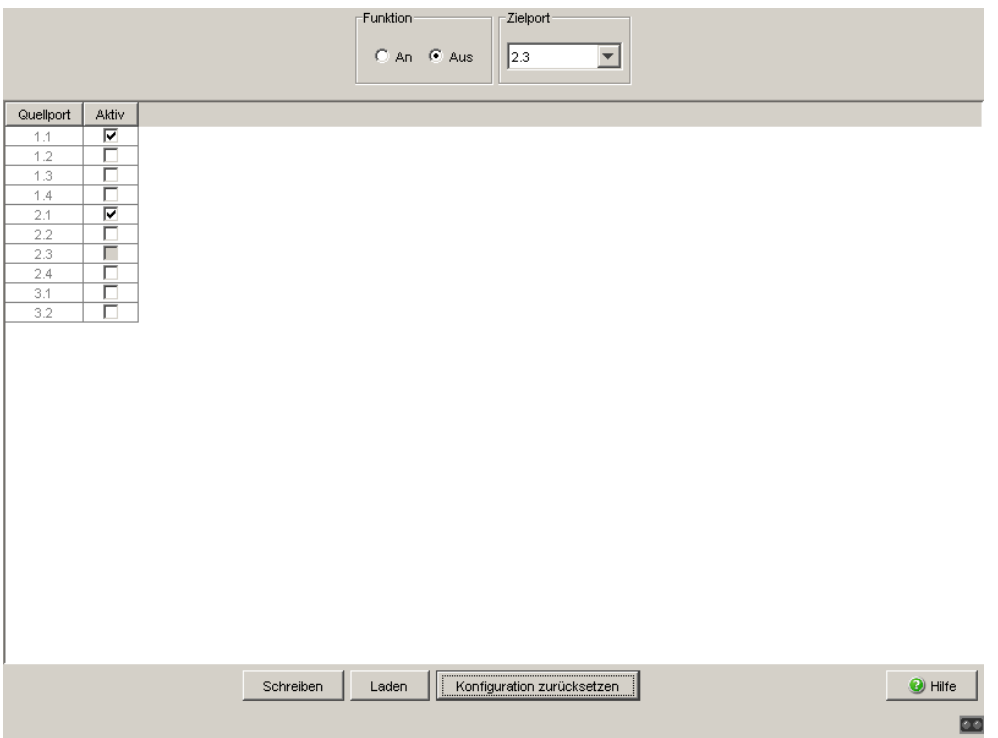


Figure 54: Port Mirroring dialog

9.12 Syslog

9.13 Event Log

The device allows you to call up a log of the system events. The table of the “Event Log” dialog lists the logged events with a time stamp.

- ☐ Click on “Load” to update the content of the event log.
- ☐ Click on “Delete” to delete the content of the event log.

Note: You have the option to also send the logged events to one or more syslog servers (see page 187 “Syslog“).

A Setting up the Configuration Environment

A.1 Setting up a DHCP/BOOTP Server

On the CD-ROM supplied with the device you will find the software for a DHCP server from the software development company IT-Consulting Dr. Herbert Hanewinkel. You can test the software for 30 calendar days from the date of the first installation, and then decide whether you want to purchase a license.

☐ To install the DHCP servers on your PC,
put the CD-ROM in the CD drive of your PC and
under Additional Software select "haneWIN DHCP-Server".
To carry out the installation, follow the installation assistant.

☐ Start the `DHCP Server` program.

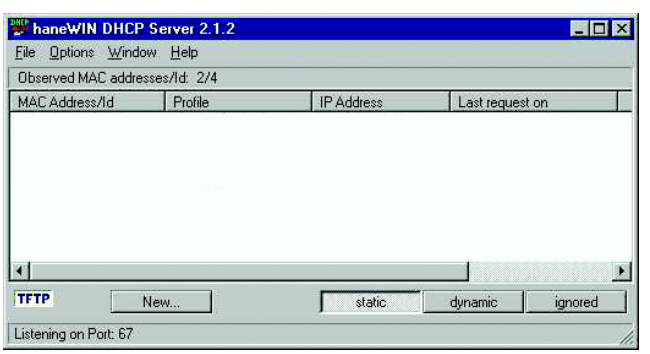


Figure 55: Start window of the DHCP server

Note: The installation procedure includes a service that is automatically started in the basic configuration when Windows is activated. This service is also active if the program itself has not been started. When started, the service responds to DHCP queries.

☐ Open the window for the program settings in the menu bar:
`Options:Preferences` and select the `DHCP` tab page.

☐ Enter the settings shown in the illustration and click `OK`.

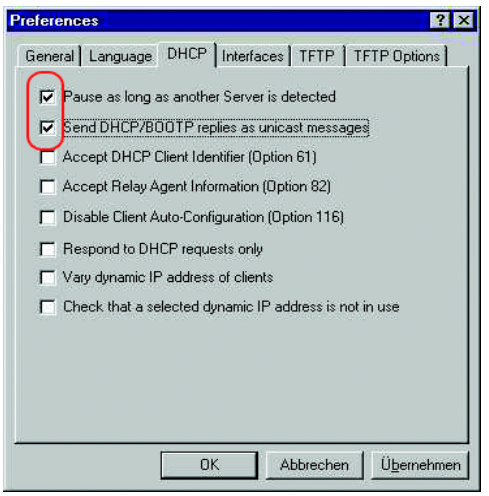


Figure 56: DHCP setting

☐ To enter the configuration profiles, select `Options:Configuration Profiles` in the menu bar.
☐ Enter the name of the new configuration profile and click `Add`.

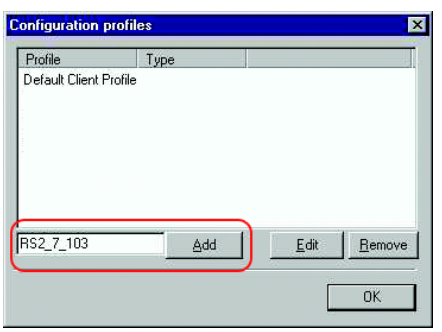


Figure 57: Adding configuration profiles

☐ Enter the network mask and click `Accept`.

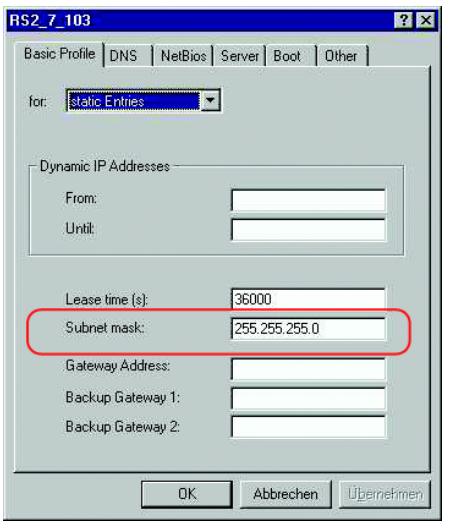


Figure 58: Network mask in the configuration profile

☐ Select the `Boot` tab page.
☐ Enter the IP address of your tftp server.
☐ Enter the path and the file name for the configuration file.
☐ Click `Apply` and then `OK`.

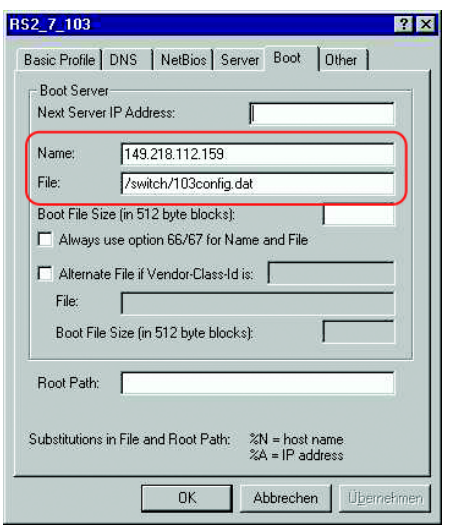


Figure 59: Configuration file on the tftp server

☐ Add a profile for each device type.
If devices of the same type have different configurations, then you add a profile for each configuration.
To complete the addition of the configuration profiles, click `OK`.

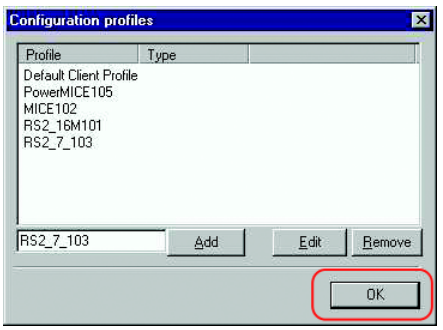


Figure 60: Managing configuration profiles

☐ To enter the static addresses, click `Static` in the main window.

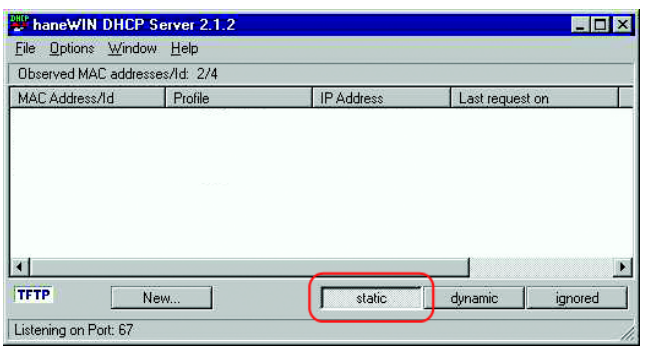


Figure 61: Static address input

☐ Click `New`.

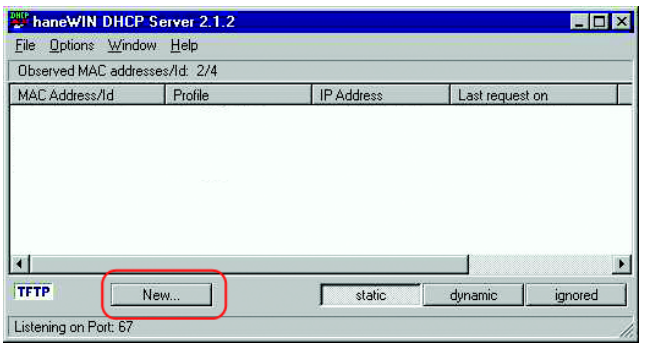


Figure 62: Adding static addresses

☐ Enter the MAC address of the device.
☐ Enter the IP address of the device.
☐ Select the configuration profile of the device.
☐ Click `Apply` and then `OK`.

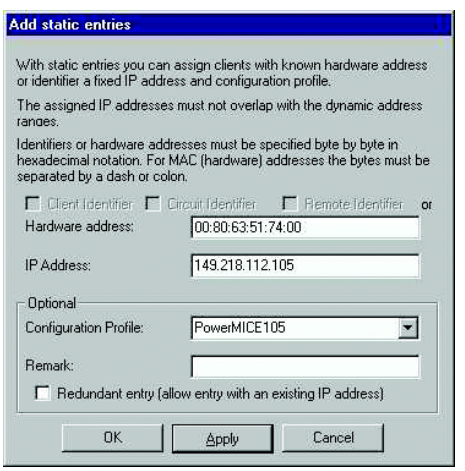

Add static entries
With static entries you can assign clients with known hardware address or identifier a fixed IP address and configuration profile.
The assigned IP addresses must not overlap with the dynamic address ranges.
Identifiers or hardware addresses must be specified byte by byte in hexadecimal notation. For MAC (hardware) addresses the bytes must be separated by a dash or colon.
Client Identifier
Circuit Identifier
Remote Identifier
or
Hardware address:
00:80:63:51:74:00
IP Address:
149.218.112.105
Optional
Configuration Profile:
PowerMICE105
Remark:
Redundant entry (allow entry with an existing IP address)
OK
Apply
Cancel

Figure 63: Entries for static addresses

☐ Add an entry for each device that will get its parameters from the DHCP server.

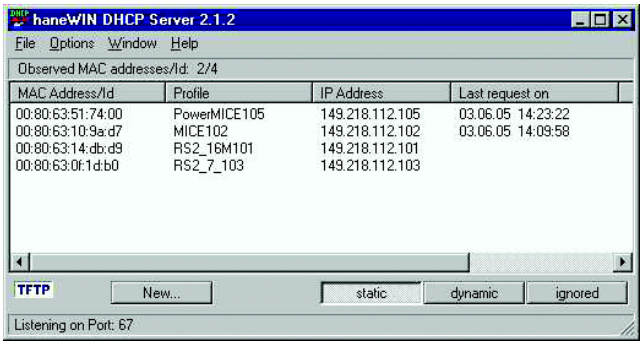


Figure 64: DHCP server with entries

A.2 Setting up a DHCP Server with Option 82

On the CD-ROM supplied with the device you will find the software for a DHCP server from the software development company IT-Consulting Dr. Herbert Hanewinkel. You can test the software for 30 calendar days from the date of the first installation, and then decide whether you want to purchase a license.

☐ To install the DHCP servers on your PC,
put the CD-ROM in the CD drive of your PC and
under Additional Software select "haneWIN DHCP-Server".
To carry out the installation, follow the installation assistant.

☐ Start the `DHCP Server` program.

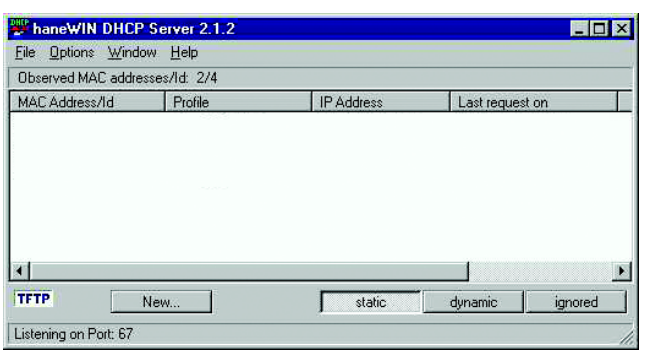


Figure 65: Start window of the DHCP server

Note: The installation procedure includes a service that is automatically started in the basic configuration when Windows is activated. This service is also active if the program itself has not been started. When started, the service responds to DHCP queries.

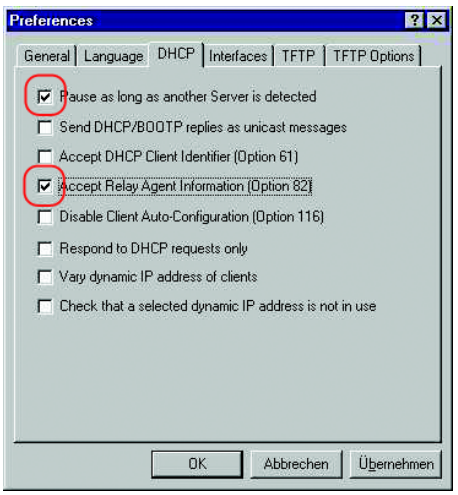


Figure 66: DHCP setting

☐ To enter the static addresses, click `New`.

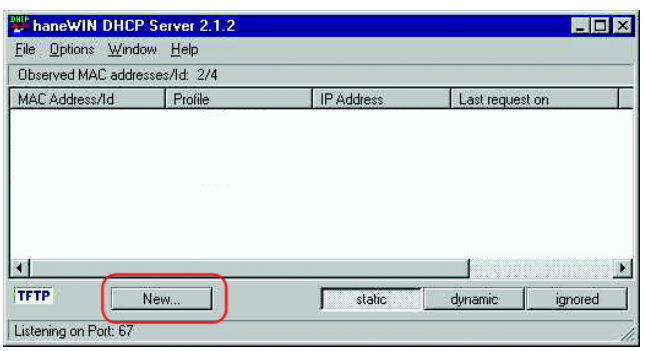


Figure 67: Adding static addresses

☐ Select `Circuit Identifier` and **Remote Identifier**.

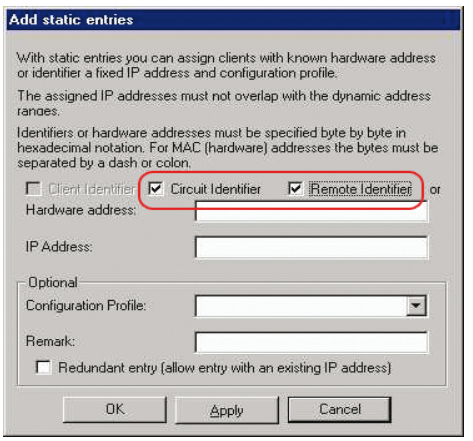

Add static entries
With static entries you can assign clients with known hardware address or identifier a fixed IP address and configuration profile.
The assigned IP addresses must not overlap with the dynamic address ranges.
Identifiers or hardware addresses must be specified byte by byte in hexadecimal notation. For MAC (hardware) addresses the bytes must be separated by a dash or colon.
Client Identifier
Circuit Identifier
Remote Identifier
or
Hardware address:
IP Address:
Optional
Configuration Profile:
Remark:
Redundant entry (allow entry with an existing IP address)
OK
Apply
Cancel

Figure 68: Default setting for the fixed address assignment

☐ In the `Hardware address` field, you enter the `Circuit Identifier` and the `Remote Identifier` (see "DHCP Relay Agent" in the "Web-based Interface" reference manual).
With `Hardware address` you identify the device and the port to which that device is connected, to which you want the assign the `IP address` in the line below it.

The hardware address is in the following form:

ciclhhvvvvssmmpprirlxxxxxxxxxxxx

- ci: sub-identifier for the type of the circuit ID
- cl: length of the circuit ID
- hh: Hirschmann ID: 01 if a Hirschmann device is connected to the port, otherwise 00.
- vvvv: VLAN ID of the DHCP request (default: 0001 = VLAN 1)
- ss: socket of device at which the module with that port is located to which the device is connected. Enter the value 00.
- mm: module with the port to which the device is connected.
- pp: port to which the device is connected.
- ri: sub-identifier for the type of the remote ID
- rl: length of the remote ID
- xxxxxxxxxxxx: remote ID of the device (e.g. MAC address) to which a device is connected.

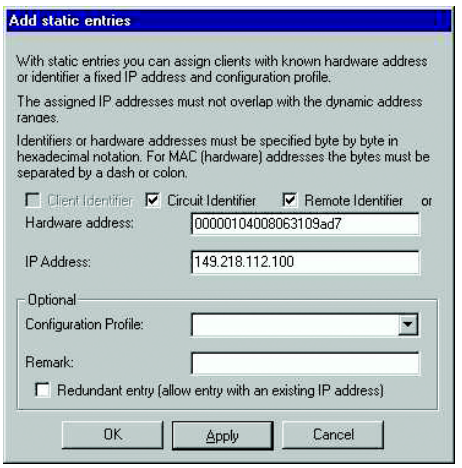

Add static entries
With static entries you can assign clients with known hardware address or identifier a fixed IP address and configuration profile.
The assigned IP addresses must not overlap with the dynamic address ranges.
Identifiers or hardware addresses must be specified byte by byte in hexadecimal notation. For MAC (hardware) addresses the bytes must be separated by a dash or colon.
Client Identifier
Circuit Identifier
Remote Identifier
or
Hardware address:
00000104008063109ad7
IP Address:
149.218.112.100
Optional
Configuration Profile:
Remark:
Redundant entry (allow entry with an existing IP address)
OK
Apply
Cancel

Figure 69: Entering the addresses

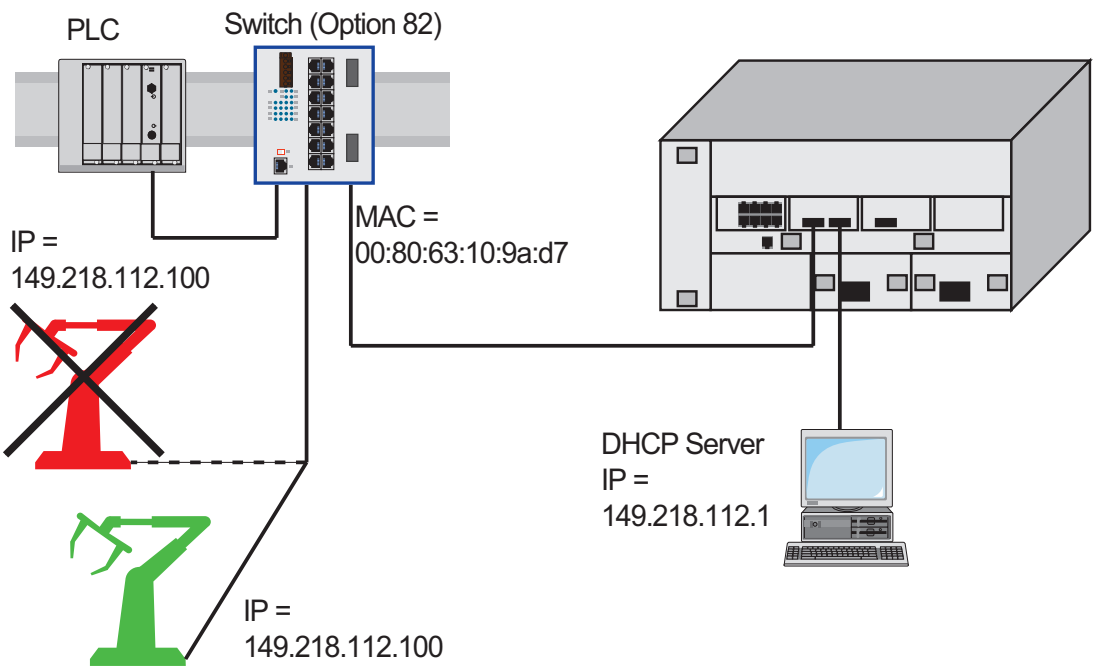


Figure 70: Application example of using Option 82

A.3 TFTP Server for Software Updates

On delivery, the device software is held in the local flash memory. The device boots the software from the flash memory.
Software updates can be performed via a tftp server. This presupposes that a tftp server has been installed in the connected network and that it is active.

Note: An alternative to the tftp update is the http update. The http update saves you having to configure the tftp server.

The device requires the following information to be able to perform a software update from the tftp server:
- its own IP address (entered permanently),
- the IP address of the tftp server or of the gateway to the tftp server,
- the path in which the operating system of the tftp server is kept

The file transfer between the device and the tftp server is performed via the Trivial File Transfer Protocol (tftp).

The management station and the tftp server may be made up of one or more computers.

The preparation of the tftp server for the device software involves the following steps:
- Setting up the device directory and copying the device software
- Setting up the tftp process

A.3.1 Setting up the tftp Process

General prerequisites:

- The local IP address of the device and the IP address of the tftp server or the gateway are known to the device.
- The TCP/IP stack with tftp is installed on tftp server.

The following sections contain information on setting up the tftp process, arranged according to operating system and application.

SunOS and HP

☐ First check whether the tftp daemon (background process) is running, i.e. whether the file /etc/inetd.conf contains the following line (see fig. 71) and whether the status of this process is "IW":

SunOS

```
tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -
s /tftpboot
```

HP

```
tftp dgram udp wait root /usr/etc/in.tftpd tftpd
```

If the process is not entered or only entered as a comment line (#), modify /etc/inetd.conf accordingly and then re-initialize the INET daemon. This is performed with the command "kill -1 PID", where PID is the process number of inetd.
This re-initialization can be executed automatically by entering the following UNIX commands:

SunOS

```
ps -ax | grep inetd | head -1 | awk -e {print $1} |
kill -1
```

HP

```
/etc/inetd -c
```

You can obtain additional information about the tftpd daemon tftpd with the UNIX command "man tftpd".

Note: The command "`ps`" does not always show the tftp daemon, although it is actually running.

Special steps for HP workstations:

☐ During installation on an HP workstation, enter the user tftp in the /etc/passwd file.

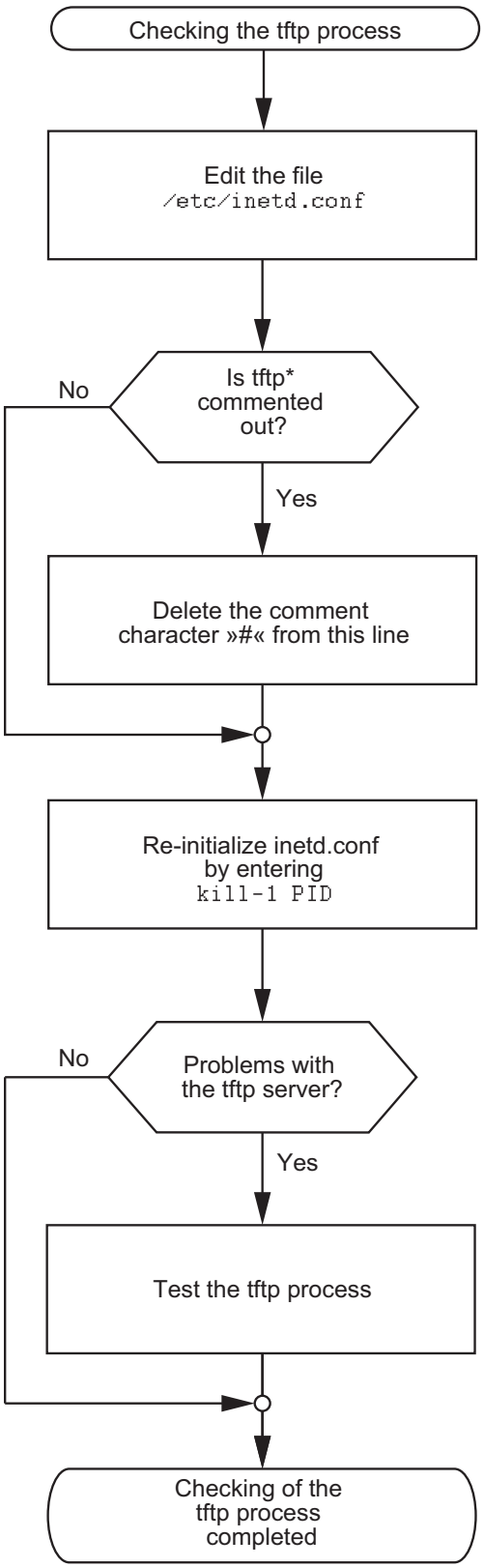
For example:

```
tftp:*:510:20:tftp server:/usr/tftpdir:/bin/false
```

`tftp`user ID,
`*` is in the password field,
`510` sample user number,
`20` sample group number.,
`tftp server` any meaningful name ,
`/bin/false` mandatory entry (login shell)

☐ Test the tftp process with, for example:`cd /tftpboot/device`

```
tftp <tftp-Servername>
get device/device.bin
rm device.bin
```



e.g
`cd /tftpboot/device`
`tftp <tftp-Servername>`
`get device/device.bin`

Response if the process is running: `Received ...`

`rm device.bin`

* `tftp dgram udp wait root/usr/etc/in.tftpd in.tftpd /tftpboot`

Figure 71: Flow chart for setting up tftp server with SunOS and HP

A.3.2 Software Access Rights

The agent needs read permission for the tftp directory on which the device software is stored.

Example of a UNIX tftp Server

Once the device software has been installed, the tftp server should have the following directory structure with the stated access rights:

File name	Access
device.bin	-rw-r--r--

Table 23: Directory structure of the software

l = link; d = directory; r = read; w = write; x = execute
1st position denotes the file type (- = normal file),
2nd to 4th positions designate user access rights,
5th to 7th positions designate access rights for users from other groups,
8th to 10th positions designate access rights of all other users.

B General Information

B.1 Management Information Base (MIB)

The Management Information Base (MIB) is designed in the form of an abstract tree structure.
The branching points are the object classes. The "leaves" of the MIB are called generic object classes.
If this is required for unique identification, the generic object classes are instantiated, i.e. the abstract structure is mapped onto reality, by specifying the port or the source address.
Values (integers, time ticks, counters or octet strings) are assigned to these instances; these values can be read and, in some cases, modified. The object description or object ID (OID) identifies the object class. The subidentifier (SID) is used to instantiate them.

Example:
The generic object class
`hmPSState (OID = 1.3.6.1.4.1.248.14.1.2.1.3)`
is the description of the abstract information "power supply status". However, it is not possible to read any information from this, as the system does not know which power supply is meant.
Specifying the subidentifier (2) maps this abstract information onto reality (instantiates it), thus indicating the operating status of power supply 2. A value is assigned to this instance and can then be read. The instance "get `1.3.6.1.4.1.248.14.1.2.1.3.2`" returns the response "1", which means that the power supply is ready for operation.

The following abbreviations are used in the MIB:	
Comm	Group access rights
con	Configuration
Descr	Description
Fan	Fan
ID	Identifier
Lwr	Lower (e.g. threshold value)
PS	Power supply
Pwr	Power supply
sys	System
UI	User interface
Upr	Upper (e.g. threshold value)
ven	Vendor = manufacturer (Hirschmann)

Definition of the syntax terms used:	
Integer	An integer in the range -2^{31} - 2^{31}-1
IP Address	xxx.xxx.xxx.xxx (xxx = integer in the range 0-255)
MAC Address	12-digit hexadecimal number in accordance with ISO/IEC 8802-3
Object identifier	x.x.x.x… (e.g. 1.3.6.1.1.4.1.248…)
Octet string	ASCII character string
PSID	Power supply identifier (number of the power supply unit)
TimeTicks	Stopwatch, Elapsed time (in seconds) = numerical value / 100 Numerical value = integer in range 0-2^{32}-1
Timeout	Time value in hundredths of a second Time value = integer in range 0-2^{32}-1
Type field	4-digit hexadecimal number in accordance with ISO/IEC 8802-3
Counter	Integer (0-2^{32-1}), whose value is increased by 1 when certain events occur.

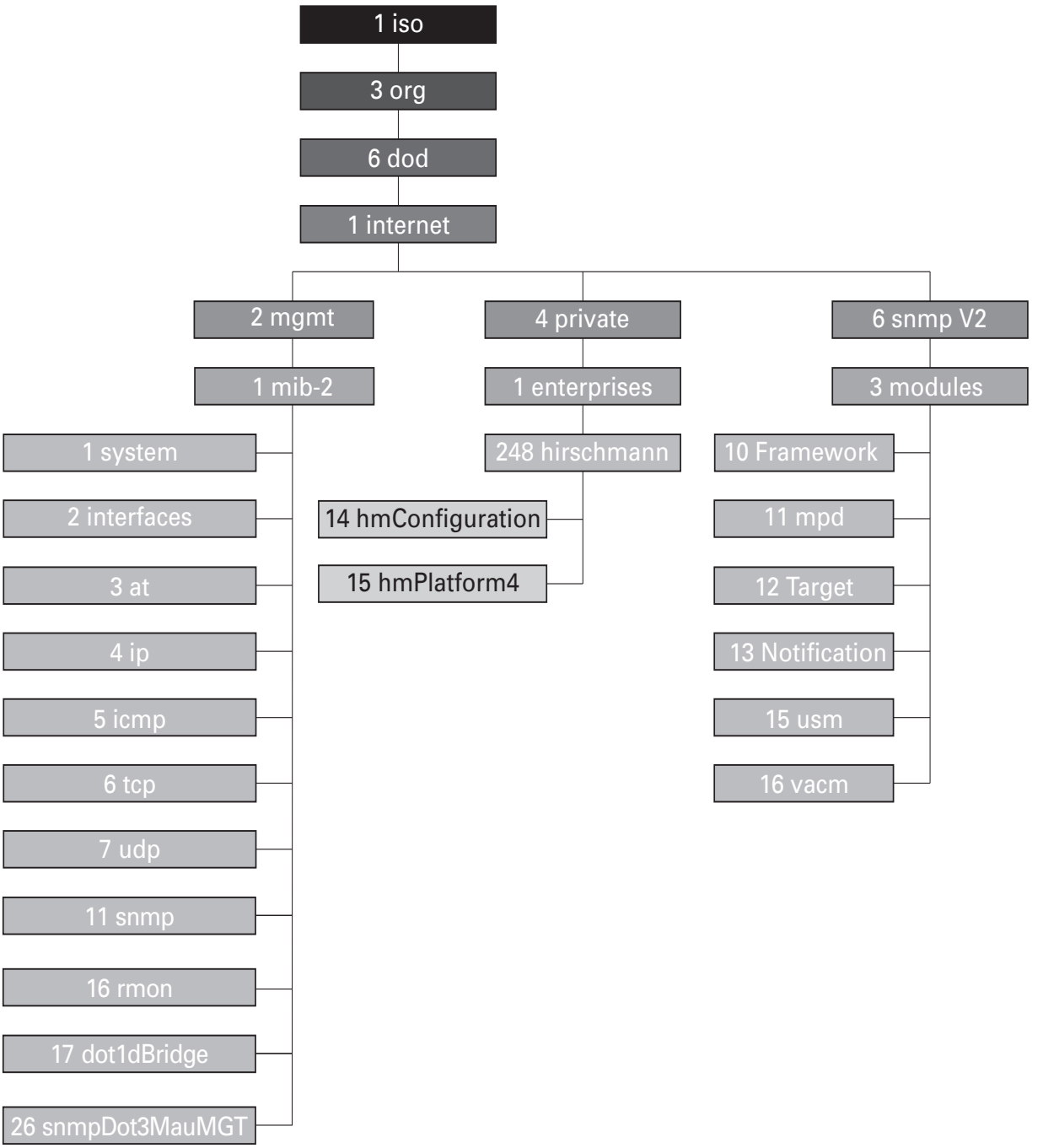


Figure 72: Tree structure of the Hirschmann MIB

A complete description of the MIB can be found on the CD-ROM included with the device.

B.2 Abbreviations used

ACA	AutoConfiguration Adapter
ACL	Access Control List
BOOTP	Bootstrap Protocol
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
FDB	Forwarding Database
GARP	General Attribute Registration Protocol
GMRP	GARP Multicast Registration Protocol
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IP	Internet Protocoll
LED	Light Emitting Diode
LLDP	Link Layer Discovery Protocol
F/O	Optical Fiber
MAC	Media Access Control
MSTP	Multiple Spanning Tree Protocol
NTP	Network Time Protocol
PC	Personal Computer
PTP	Precision Time Protocol
QoS	Quality of Service
RFC	Request For Comment
RM	Redundancy Manager
RS	Rail Switch
RSTP	Rapid Spanning Tree Protocol
SFP	Small Form-factor Pluggable
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TP	Twisted Pair
UDP	User Datagramm Protocol
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
VLAN	Virtual Local Area Network

B.3 Technical Data

You will find the technical data in the document „Reference Manual Web-based Interface“.

B.4 Readers' Comments

What is your opinion of this manual? We are always striving to provide as comprehensive a description of our product as possible, as well as important information that will ensure trouble-free operation. Your comments and suggestions help us to further improve the quality of our documentation.

Your assessment of this manual:

	Very good	Good	Satisfactory	Mediocre	Poor
Precise description	O	O	O	O	O
Readability	O	O	O	O	O
Understandability	O	O	O	O	O
Examples	O	O	O	O	O
Structure	O	O	O	O	O
Completeness	O	O	O	O	O
Graphics	O	O	O	O	O
Drawings	O	O	O	O	O
Tables	O	O	O	O	O

Did you discover any errors in this manual?
If so, on what page?

Suggestions for improvement and additional information:

General comments:

Sender:

Company / Department:

Name / Telephone number:

Street:

Zip code / City:

E-mail:

Date / Signature:

Dear User,

Please fill out and return this page

- as a fax to the number +49 (0)7127/14-1600 or
- by mail to

  Hirschmann Automation and Control GmbH
  Department AED
  Stuttgarter Str. 45-51
  72654 Neckartenzlingen

C Index

A

ACA 37, 52, 63, 65, 158, 158, 158
Access 158
Access right 58
Access rights 77
Access security 71
Access with Web-based interface, password 78
ACD 178
Address conflict 178
Address Conflict Detection 178
Address table 105
AF 125
Aging Time 105, 105
Aging time 110, 110
Alarm 157
Alarm messages 154
APNIC 25
ARIN 25
ARP 29
Assured Forwarding 125
Authentication 158
AutoConfiguration Adapter 37, 158, 158
Automatic configuration 71

B

Bandwidth 108, 132
Booting 14
BOOTP 23, 44, 52
Broadcast 104, 106, 108
Broadcast Limiter Settings 119
Browser 19

C

CD-ROM 190, 196
CIDR 30
Class Selector 125
Classless Inter Domain Routing 30
Classless Inter-Domain Routing 29
CLI access, password 78
Clock 98
Clock synchronization 100
Closed circuit 162
Cold start 65
Command Line Interface 16
Configuration 56
Configuration changes 154
Configuration data 39, 47, 54, 57
Configuration file 44, 53
Connection error 72

D

Data transfer parameter 14
Destination address 106, 106, 107
Destination address field 105
Destination table 154
Device Status 159, 159, 162
Device status 159
DHCP 23, 44, 44, 47, 52
DHCP Client 44
DHCP client 44
DHCP Option 82 47, 190, 196
DHCP server 90, 190, 196
Differentiated Services 125
DiffServ 121
DiffServ-Codepoint 125
DSCP 125, 127, 129, 130
Dynamic 106

E

EF 125
Event log 188
Expedited Forwarding 125

F

FAQ 217
Faulty device replacement 50
FDB 106
Filter 106
Filter table 106
First installation 23
Flash memory 56, 65
Flow control 132, 132
Forwarding database 106

G

Gateway 26, 32
Generic object classes 206
GMRP 108
Grandmaster 98

H

HaneWin 190, 196
Hardware address 40
Hardware reset 154
HiDiscovery 34, 83, 83
HIPER-Ring 7
HIPER-Ring (source for alarms) 158

HiVision 8, 45
Host address 26

i
in-band 16

I
IANA 25
IEEE 1588 time 90
IEEE 802.1 Q 122
IEEE MAC address 174
IGMP 110
IGMP Querier 112
IGMP Snooping 108, 110, 110
Industry Protocols 7
Instantiation 206
Internet Assigned Numbers Authority 25
Internet service provider 25
IP Address 44
IP address 25, 32, 40, 178
IP header 121, 124
IP Parameter 23
IP Parameters (device network settings) 48
IP- Header 125
ISO/OSI layer model 29

J
Java 20
Java Runtime Environment 19
JavaScript 20

L
LACNIC 25
Leave 110, 110
Link monitoring 159, 162
LLDP 176
Local clock 99
Login 20

M
MAC destination address 29
Media module (for modular devices) 158
Message 154
MRP 7
Multicast 95, 106, 108, 110

N
Netmask 26, 32
Network address 25
Network Management 45
Network Management Software 8
Network topology 47
NTP 92, 94

O
Object classes 206
Object description 206
Object ID 206
Operating mode 71
Operation monitoring 162
Option 82 24, 47, 196
Overload protection 132

o
out-of-band 16

P
Password 17, 20, 58, 79
Password for access with Web-based interface 78
Password for CLI access 78
Password for SNMPv3 access 78
PHB 125
Polling 154
Port configuration 71
Port Mirroring 184
Port mirroring 185
Port priority 127
Power over ETHERNET 72
Precedence 125
Precision Time Protocol 89, 98
Priority 122, 127
Priority queues 121
Priority tagged frames 122
PROFINET IO 7
PTP 89, 90, 98
PTP subdomains 100

Q
QoS 121
Query 110
Query function 112
Queue 128

R
Rate Limiter Settings 119
Read access 20
Real time 89, 121
Reboot 65
Receiver power status 158
Receiving port 107
Redundancy 7
Reference clock 90, 93, 98
Relay contact 162
Release 61
Remote diagnostics 162
Report 110, 182
Request interval (SNTP) 95

Reset 65
Restart 65
Ring manager 106
Ring/Network Coupling 7
Ring/Network coupling (source for alarms) 158
RIPE NCC 25
RMON probe 184
Router 26

S

Segmentation 154
Service 182
Service provider 25
SFP module 172
SFP Module (source for alarms) 158
SFP status display 172
Signal contact 72, 162
Signal contact (source for alarm) 158
Signal runtime 93
Simple Network Time Protocol 89
SNMP 19, 77, 154
SNMPv3 access, password 78
SNTP 89, 92, 94
SNTP client 92, 95, 96
SNTP server 92
Software 204
Software release 61
Source address 104
State on deliver 56
State on delivery 56, 77
Static 106
Strict Priority 127, 128
Subdomains 100
Subidentifier 206
Subnetwork 32, 105
Summer time 90
Supply voltage 158
Symbol 9
System Monitor 14, 14
System Name 44
System name 44
System time 93, 95

T

TCP/IP stack 201
Technical questions 217
Telnet 16
Time difference 90
Time management 98
Time zone 90
Topology 47, 176
ToS 121, 124, 125
Traffic class 127, 129, 129
Traffic classes 121
Training courses 217
Transmission reliability 154
Trap 154, 157
Trap Destination Table 154
Trivial File Transfer Protocol 200
Type Field 122
Type of Service 124

t

tftp 200
tftp update 69
trust dot1p 127
trust ip-dscp 127

u

untrusted 127

U

Unicast 108
Universal Time Coordinated 92
Update 14
USB stick 63
User name 17
UTC 90, 92

V

V.24 16, 16
Video 128
VLAN 122, 127, 135
VLAN ID (device network settings) 48
VLAN priority 129
VLAN Tag 122
VLAN tag 122, 135
VoIP 128

W

Web-based Interface 19
Web-based interface 19
Web-based management 20
Website 21
Winter time 90
Write access 20

D Further Support

Technical Questions and Training Courses

In the event of technical queries, please contact your local Hirschmann distributor or Hirschmann office.
You can find the addresses of our distributors on the Internet: www.hirschmann-ac.com.

Our support line is also at your disposal:

- Tel. +49 1805 14-1538
- Fax +49 7127 14-1551

Answers to Frequently Asked Questions can be found on the Hirschmann internet site (www.hirschmann-ac.com) at the end of the product sites in the FAQ category.
The current training courses to technology and products can be found under http://www.hicomcenter.com.

Hirschmann Competence Center

In the long term, excellent products alone do not guarantee a successful customer relationship. Only comprehensive service makes a difference worldwide. In the current global competition scenario, the Hirschmann Competence Center is ahead of its competitors on three counts with its complete range of innovative services:

- Consulting incorporates comprehensive technical advice, from system evaluation through network planning to project planing.
- Training offers you an introduction to the basics, product briefing and user training with certification.
- Support ranges from the first installation through the standby service to maintenance concepts.

With the Hirschmann Competence Center, you have decided against making any compromises. Our client-customized package leaves you free to choose the service components you want to use.
Internet:
http://www.hicomcenter.com.

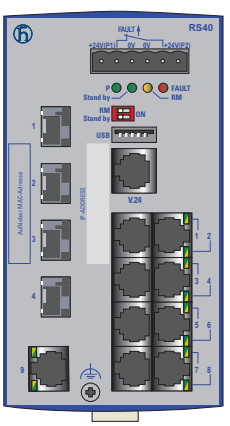
HIRSCHMANN

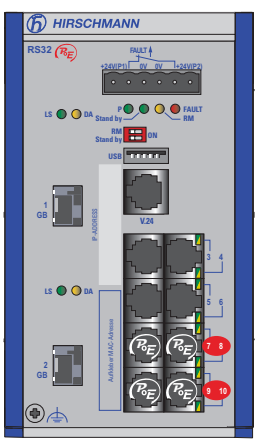
A BELDEN BRAND

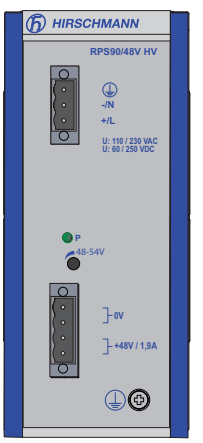
HIRSCHMANN
A BELDEN BRAND

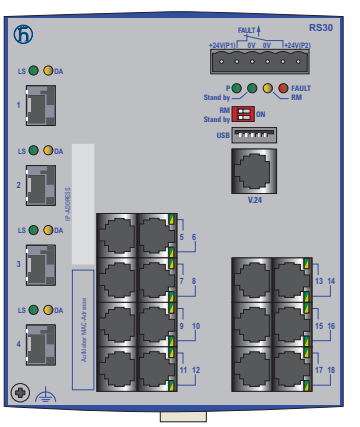
User Manual

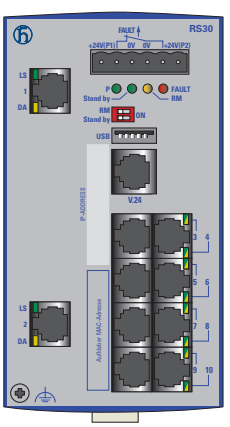
Installation
Industrial ETHERNET Rail Switch
RS20/RS22/RS30/RS32/RS40 Family

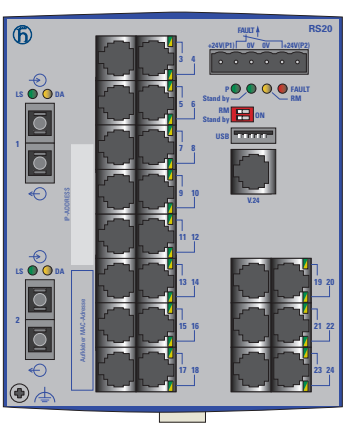

RS40-0009...

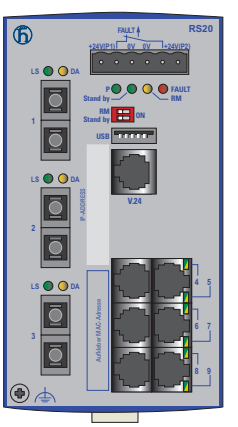

RS32-0802...

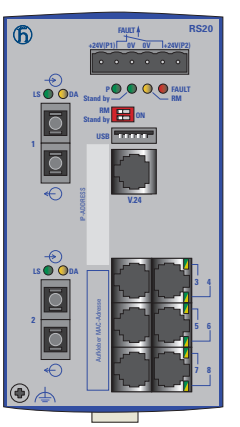

RPS90/48V HV

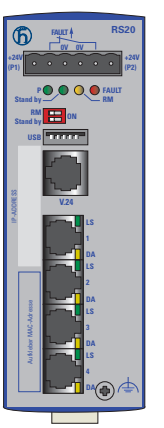

RS30-1602...


RS30-0802...


RS20-2400...


RS20-0900...


RS20-0800...


RS20-0400...

03692002171010000

Technical Support
HAC.Support@Belden.com

The naming of copyrighted trademarks in this manual, even when not specially indicated, should not be taken to mean that these names may be considered as free in the sense of the trademark and tradename protection law and hence that they may be freely used by anyone.

© 2010 Hirschmann Automation and Control GmbH

Manuals and software are protected by copyright. All rights reserved. The copying, reproduction, translation, conversion into any electronic medium or machine scannable form is not permitted, either in whole or in part. An exception is the preparation of a backup copy of the software for your own use. For devices with embedded software, the end-user license agreement on the enclosed CD applies.

The performance features described here are binding only if they have been expressly agreed when the contract was made. This document was produced by Hirschmann Automation and Control GmbH according to the best of the company's knowledge. Hirschmann reserves the right to change the contents of this document without prior notice. Hirschmann can give no guarantee in respect of the correctness or accuracy of the information in this document.

Hirschmann can accept no responsibility for damages, resulting from the use of the network components or the associated operating software. In addition, we refer to the conditions of use specified in the license contract.

You can get the latest version of this manual on the Internet at the Hirschmann product site (www.beldensolutions.com).

Printed in Germany
Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Germany
Tel.: +49 1805 141538

Contents

Safety instructions 4

About this Manual 11

Key 11

1 Device description 12

1.1 Description of the device variants 14
1.1.1 Combination options for RS20/30 16
1.1.2 Combination options for RS40 19
1.1.3 Number of ports and media for RS20-... 20
1.1.4 Number of ports and media for RS30-... 24
1.1.5 Number of ports and media for RS40-... 27

1.2 Device variants with PoE (optional) 28
1.2.1 Number of ports and media for devices with PoE 28
1.2.2 PoE power units 30

2 Assembly and start-up 31

2.1 Installing the device 31
2.1.1 Unpacking and checking 31
2.1.2 Installing the SFP modules (optional) 32
2.1.3 Insert data in label area 32
2.1.4 Adjust DIP switch settings 33
2.1.5 RS20/RS30/RS40: supply voltage and signal contact 33
2.1.6 RS22/RS32: supply voltage and signal contact 35
2.1.7 Installing the device on the DIN rail, grounding 38
2.1.8 Dimension drawings 41
2.1.9 Connecting the ferrite 44
2.1.10 Installing the terminal block, start-up procedure 44
2.1.11 Connecting the data lines 44

2.2 Display elements 48

2.3 Basic set-up 50

2.4 Disassembly 52

3 Technical data 53

A Further Support 63

Safety instructions

Notes on safety

This manual contains instructions to be observed for ensuring your personal safety and for preventing damage. The warnings appear next to a warning triangle with a different heading depending on the degree of danger posed:

Danger!
Means that death, serious physical injury or significant damage to property **will occur** if the corresponding safety measures are not carried out.

Warning!
Means that death, serious physical injury or significant damage to property **could occur** if the corresponding safety measures are not carried out.

Caution!
Means that minor physical injury or damage to property can occur if the required safety measures are not carried out.

Note: Contains important information on the product, on how to manage the product, or on the respective section of the documentation to which your special attention is being drawn.

Certified usage

Please observe the following: The device may only be employed for the purposes described in the catalog and technical description, and only in conjunction with external devices and components recommended or approved by the manufacturer. The product can only be operated correctly and safely if it is transported, stored, installed and assembled properly and correctly. Furthermore, it must be operated and serviced carefully.

Supply voltage

For safety reasons the devices have been designed to operate at low voltages. Thus, they may only be connected to the supply voltage connections and to the signal contact with SELV circuits with the voltage restrictions in accordance with IEC/EN 60950-1.
The supply voltage is electrically isolated from the housing.
☐ Use undamaged parts.

☐ Relevant for North America: For use in Class 2 circuits.
The device may only be connected to a supply voltage of class 2 that fulfills the requirements of the National Electrical Code, Table 11(b). If the voltage is being supplied redundantly (two different voltage sources), the combined supply voltages must fulfill the requirements of the National Electrical Code, Table 11(b).

☐ Relevant for North America: For use in Class 2 circuits.
Only use copper wire/conductors of class 1, 75 °C (167 °F).

☐ Relevant for North America
for devices certified for hazardous locations:
Power, input and output (I/O) wiring must be in accordance with Class I, Division 2 wiring methods [Article 501-4(b) of the National Electrical Code, NFPA 70] and in accordance with the authority having jurisdiction.

☐ Relevant for RS20 devices and RS30 devices used in explosive gas atmospheres according to ATEX Directive 94/9 EC:
- ▶ Make sure that the device has the following label:
  ⟨Ex⟩ II 3G (... followed by other specifications).
- ▶ The product must be mounted in a suitable IP 54-certified housing – tested to 4 J impact to minimize the risk of mechanical damage.
- ▶ For ambient temperatures below -10 °C and above +60 °C use wiring suitable for both the minimum and maximum temperatures.
- ▶ Connectors may be connected exclusively in dead-voltage state.
- ▶ DIP switches may be switched exclusively in dead-voltage state.

☐ The device does not contain any service components. Internal fuses are only triggered if there is a fault in the device. If the device is not functioning correctly, or if it is damaged, switch off the voltage supply and return the device to the plant for inspection.

☐ Only switch on the supply voltage to the device if
- the housing is closed,
- the terminal blocks are wired up correctly and
- the terminal blocks are connected.

Supply voltage for PoE power supply units (optional)

☐ Connect the protective conductor with the ground screw before you set up the other connections. When removing the connections, you remove the protective conductor last.

☐ Make sure that the cross-section of the protective conductor cable is the same size as or bigger than the cross-section of the voltage supply cables.

☐ Only use connection cables that are permitted for the specified temperature range.

Warning!
- If the neutral conductor or the negative terminal of the supply voltage is not grounded
- If you are using a DC voltage greater than 125 V DC for the supply voltage install a suitable input fuse.

For RPS90/48V-LV power supply units, use a slow-blow fuse with a nominal rating of 10 A for the voltage supply input.
For RPS90/48V-HV power supply units, use a slow-blow fuse with a nominal rating of 6.3 A.
With AC power supply, use a cable cross-section of at least 0.75 mm² (for North America AWG 18) for the current conductor at the voltage input.
With DC power supply, use a cable cross-section of at least 1.0 mm² (for North America AWG 16) for the current conductor at the voltage input.

Warning!
Only connect a supply voltage that corresponds to the type plate of your device.

- PoE power supply unit RPS90/48V LV:18 V DC to 60 V DC
- PoE power supply unit RPS90/48V HV:48 V DC to 320 V DC or 90 V AC to 265 V AC

Shielding ground

Note: The shielding ground of the connectable twisted pair lines is connected to the front panel as a conductor.

☐ Beware of possible short circuits when connecting a cable section with conductive shielding braiding.

ATEX Directive 94/9 EC

Relevant for RS40 devices devices used in explosive gas atmospheres according to ATEX Directive 94/9 EC:

☐ Make sure that the device has the following label:
II 3G (... followed by other specifications)

☐ The modules shall be installed in an enclosure in accordance with EN 60079-15 providing a degree of protection of at least IP54 according to EN 60529, taking into account the environmental conditions under which the equipment will be used.

☐ When the temperature under rated conditions exceeds 70 °C at the cable or conduit entry point, or 80 °C at the branching point of the conductors, the temperature specification of the selected cable shall be in compliance with the actual measured temperature values.

☐ Provisions shall be made to prevent the rated voltage from being exceeded by transient disturbances of more than 40%.

Housing

Warning!
Never insert sharp objects (small screwdrivers, wires, etc.) into the inside of the product. There is the risk of an electric shock.

Warning!
When installing the device, make sure the ventilation slots remain free, as otherwise damage can occur through overheating.

Only technicians authorized by the manufacturer are permitted to open the housing.
The housing is grounded via the separate ground screw on the bottom left of the front panel.

For the ground conductor, use a cable with a cross section of at least 1.0 mm².

☐ The clearance to the ventilation slots of the housing must be at least 10 cm (3.94 in).

☐ The device must be installed in the vertical position.
☐ If installed in a living area or office environment, the device must be operated exclusively in switch cabinets with fire protection characteristics in accordance with EN 60950-1.

Environment

The device may only be operated at the specified surrounding air temperature (temperature of the surrounding air at a distance of up to 5 cm (1.97 in) from the device) and relative air humidity specified in the technical data.
☐ Install the device in a location where the climatic threshold values specified in the technical data will be observed.
☐ Use the device only in an environment within the contamination level specified in the technical data.

Qualification requirements for personnel

Qualified personnel as understood in this manual and the warning signs, are persons who are familiar with the setup, assembly, startup, and operation of this product and are appropriately qualified for their job. This includes, for example, those persons who have been:

- trained or directed or authorized to switch on and off, to ground and to label power circuits and devices or systems in accordance with current safety engineering standards;
- trained or directed in the care and use of appropriate safety equipment in accordance with the current standards of safety engineering;
- trained in providing first aid.

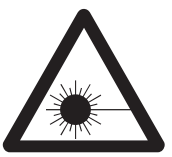
General safety instructions

Electricity is used to operate this equipment. Comply with every detail of the safety requirements specified in the operating instructions regarding the voltages to apply (see page 4).

Non-observance of these safety instructions can therefore cause material damage and/or serious injuries.

- ☐ Only appropriately qualified personnel should work on this device or in its vicinity. These personnel must be thoroughly familiar with all the warnings and maintenance procedures in accordance with this operating manual.
- ☐ The proper and safe operation of this device depends on proper handling during transport, proper storage and assembly, and conscientious operation and maintenance procedures.
- ☐ Never start operation with damaged components.
- ☐ Only use the devices in accordance with this manual. In particular, observe all warnings and safety-related information.
- ☐ Any work that may be required on the electrical installation may only be carried out by personnel trained for this purpose.

Note: LED or LASER components in compliance with IEC 60825-1 (2001):
CLASS 1 LASER PRODUCT
CLASS 1 LED PRODUCT



Warning
Laser light
Do not look into the beam or view it directly with optical instruments (e.g. magnifying glasses, microscopes).
Failure to observe this warning within a distance of 100 mm

can endanger your sight.
Light is emitted from the optical connections or from the ends of the optical fibers that are connected to them. Light Emitting Diode CLASS 2M, wave length 650 nm, power <2 mW, according to
DIN EN 60825-1:2003-10.

National and international safety regulations

☐ Make sure that the electrical installation meets local or nationally applicable safety regulations.

CE marking

The devices comply with the regulations contained in the following European directive(s):

2004/108/EG
Directive of the European Parliament and the council for standardizing the regulations of member states with regard to electromagnetic compatibility.

RPS90/48V HV:
2006/95/EG
Directive of the European Parliament and the council for standardizing the regulations of member states with regard to electrical equipment to be used within specific voltage ranges.

RPS90/48V LV:
72/245/EWG, 2004/104/EG, 2009/19/EGEG
Guideline for standardizing the regulations of member states relating to radio interference from motor vehicles. Certified devices are marked with an e1 type approval indicator.

In accordance with the above-named EU directive(s), the EU conformity declaration will be at the disposal of the relevant authorities at the following address:

Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Tel.: +49 1805 141538

The product can be used in living areas (living area, place of business, small business) and in industrial areas.

- Interference immunity: EN 61000-6-2:2005
- Emitted interference: EN 55022:2006 + A1:2007 Class A

Warning!
This is a class A device. This device can cause interference in living areas, and in this case the operator may be required to take appropriate measures.
The assembly guidelines provided in these instructions must be strictly adhered to in order to observe the EMC threshold values.

FCC note:

This device complies with part 15 of FCC rules. Operation is subject to the following two conditions : (1) This device may not cause harmful interference; (2) this device must accept any interference received, including interference that may cause undesired operation.
Appropriate testing has established that this device fulfills the requirements of a class A digital device in line with part 15 of the FCC regulations.
These requirements are designed to provide sufficient protection against interference when the device is being used in a business environment.
The device creates and uses high frequencies and can radiate same, and if it is not installed and used in accordance with this operating manual, it can cause radio transmission interference. The use of this device in a living area can also cause interference, and in this case the user is obliged to cover the costs of removing the interference.

Recycling note

After usage, this product must be disposed of properly as electronic waste, in accordance with the current disposal regulations of your county, state and country.

About this Manual

The “Installation” user manual contains a device description, safety instructions, a description of the display, and the other information that you need to install the device.
The following manuals are available as PDF files on the CD-ROM supplied:

- Installation user manual
- Basic Configuration user manual
- Redundancy Configuration user manual
- Web-based Interface reference guide
- Command Line Interface user manual

The Network Management Software HiVision/Industrial HiVision provides you with additional options for smooth configuration and monitoring:

- Configuration of multiple devices simultaneously.
- Graphical interface with network layouts.
- Auto-topology discovery.
- Event log.
- Event handling.
- Client / Server structure.
- Browser interface
- ActiveX control for SCADA integration
- SNMP/OPC gateway

Key

The symbols used in this manual have the following meanings:

▶	Listing
☐	Work step
■	Subheading

1 Device description

The RS20/22/30/32/40 family provides you with a range of Switch variants. You can set up your device individually based on different criteria:

- Number of ports
- Transmission speed
- Media type
- Types of connectors
- Temperature range
- Certifications
- Software variant

The RS20/22/30/32/40 devices are designed for the special requirements of industrial automation. They meet the relevant industry standards, provide very high operational reliability, even under extreme conditions, and also long-term reliability and flexibility.

The devices allow you to set up switched industrial ETHERNET networks that conform to the IEEE 802.3 and 802.3u standards using copper wires or optical fibers in a line or ring structure.

The devices work without a fan.

The voltage is supplied redundantly.

Mount the devices by

- simply snapping them onto a DIN rail
- mounting them on a wall (only RS22/RS32)

Depending on the device variant, you can choose various media to connect terminal devices and other infrastructure components:

- twisted pair cable
- multimode F/O
- singlemode F/O

The twisted pair ports support:

- Autocrossing
- Autonegotiation
- Autopolarity

There are a number of convenient options for managing the device. Administer your devices via:

- a Web browser
- Telnet
- management software (e.g. HiVision)
- a V.24 interface (locally on the Switch)

The HIPER-Ring redundancy concept enables a quick reconfiguration. With one additional connection, projection remains simple.

Product configuration data can be provided by:

- diagnosis displays
- displaying the operating parameters
- a label area for the IP address

Depending on the software you choose, the devices provide you with a large range of functions:

- Redundancy functions
  - Rapid Spanning Tree Protocol (RSTP)
  - Redundant ring structure
  - HIPER-Ring
  - Redundant coupling
  - Link aggregation
  - Redundant power supply
- Security
  - Protection from unauthorized access
  - Blocking of unauthorized messages (MAC or IP based)
- Synchronized system time in the network
- Network load control
- Operation diagnosis
- Diagnostics (hardware self-testing)
- Reset
- Priority
- VLAN
- Topology Discovery
- Web-based Interface
- Command Line Interface CLI
- SNMP
- 802.1x port authentication
- Real Time Clock

The Hirschmann network components help you to establish continuous communication across all levels of the company. Connect your devices to:

- devices of the MICE family
- backbone devices of the MACH family
- the BAT wireless transmission system
- the EAGLE security system
- products for the LION control room / MACH 100 family

1.1 Description of the device variants

The devices differ with regard to the range of software functions, the number of interfaces, and the media type for connecting segments.

The table below shows three port categories for each product variant: uplink ports, PoE ports and other ports. The table also shows for each product category the number of ports you can select, and the type of ports. In the column for the port type, the abbreviations F/O (optical fiber) and TP (twisted pair) indicate the media type, while the abbreviations DSC, ST, SFP and RJ45 indicate the socket type.

Variant	Uplink ports		Other ports		PoE ports included	
	Number	Type	Number	Type	Number	Type
RS20-...	2	Ports 1 and 2 10/100 Mbit/s, media selectable, DSC, ST, RJ45	2, 6, 14, 22	10/100 Mbit/s, TP, RJ45	—	—
	3	Ports 1 to 3 10/100 Mbit/s, media selectable, DSC, ST, RJ45	6, 14, 22	10/100 Mbit/s, TP, RJ45	—	—
RS22-...	2	Ports 1 and 2 10/100 Mbit/s, media selectable, DSC, ST, RJ45	6, 14, 22	10/100 Mbit/s, TP, RJ45	4	10/100 Mbit/s, TP, RJ45
	3	Ports 1 to 3 10/100 Mbit/s, media selectable, DSC, ST, RJ45	6, 14, 22	10/100 Mbit/s, TP, RJ45	4	10/100 Mbit/s, TP, RJ45
RS30-...	2	Ports 1 and 2 1000 Mbit/s, media selectable, SFP, RJ45	8, 16, 24	10/100 Mbit/s, TP, RJ45	—	—
	4	Ports 1+2, 3+4 2x100/1000 Mbit/s, 2x 100 Mbit/s, F/O, SFP	6, 14, 22	10/100 Mbit/s, TP, RJ45	—	—
RS32-...	2	Ports 1 and 2 1000 Mbit/s, media selectable, SFP, RJ45	8, 16, 24	10/100 Mbit/s, TP, RJ45	4	10/100 Mbit/s, TP, RJ45
	4	Ports 1+2, 3+4 2x100/1000 Mbit/s, 2x 100 Mbit/s, F/O, SFP	6, 14, 22	10/100 Mbit/s, TP, RJ45	4	10/100 Mbit/s, TP, RJ45
RS40-...	4	Ports 1 to 4 4 combo ports: 100/1000 Mbit/s, F/O, SFP 10/100/1000 Mbit/s, TP, RJ45	5	10/100/ 1000 Mbit/s, TP, RJ45	—	—

Table 1: Number and type of ports

The devices also provide you with the following options for selecting the variant you desire:

Operating temperature	Standard	0 °C to +60 °C
	Extended	-40 °C to +70 °C
	Extended with conformal coating	-40 °C to +70 °C
	Extended with PoE devices	-40 °C to +50 °C
Operating voltage	Standard	9.6 to 60 V DC or 18 to 30 V AC Safety extra-low voltage (SELV), redundant inputs disconnected.
	PoE	48 V (47 V DC to 52 V DC)
Certifications / declarations	CE, UL508, ISA 12.12.01 (UL1604)	
	CE, UL508, ISA 12.12.01 (UL1604), Germanischer Lloyd (GL), IEC/EN 61850-3 declaration (sub station), IEEE 1613 (sub station), EN 50121-4 railway (along track)	
	CE, UL508, ISA 12.12.01 (UL1604), Germanischer Lloyd (GL), IEC/EN 61850-3 declaration (sub station), IEEE 1613 (sub station), EN 50121-4 railway (along track), ATEX RL 94/9 EG (hazardous location)	
Software variant	Enhanced Professional	

The devices comply with the specifications of the standard(s):

- ISO/IEC 8802-03 10BASE-T/100BASE-TX/1000BASE-T
- ISO/IEC 8802-03 100BASE-FX
- ISO/IEC 8802-03 1000BASE-SX/LX

1.1.1 Combination options for RS20/30

The product designation of your device is made from combining the desired product characteristics in accordance with the following table. You will find the corresponding short designation in columns 3 and 4.

Item	Characteristic	Ident.	Ident. 2 [a]	Property
1 to 4	Product	RS20		Rail Switch without gigabit ports
		RS30		Rail Switch with gigabit ports
		RS22		Rail Switch without gigabit ports, with PoE [b][c]
		RS32		Rail Switch with gigabit ports, with PoE [b][c]
5	- (hyphen)	-		
6 to 7	Number of 10/100	04		4 * 10/100 Mbit/s Ethernet
	Mbit/s ports	08		8 * 10/100 Mbit/s Ethernet
		09		9 * 10/100 Mbit/s Ethernet
		16		16 * 10/100 Mbit/s Ethernet
		17		17 * 10/100 Mbit/s Ethernet
		24		24 * 10/100 Mbit/s Ethernet
		25		25 * 10/100 Mbit/s Ethernet
8 and 9	Number of 1000	00		0 * 1000 Mbit/s Ethernet
	Mbit/s ports	02		2 * 1000 Mbit/s Ethernet (not for 4-port devices) [b]
10 and 11 [a]	Uplink port(s)	T1		Twisted pair T(X), RJ45
	1 port (Ident. column)	M2	MM [d]	Multimode FX, DSC, 100 Mbit/s
	or alternatively	M4	NN [d]	Multimode FX, ST, 100 Mbit/s
	2 ports	S2	VV [d]	Singlemode FX, DSC, 100 Mbit/s
	(Ident.2 column)	S4	UU [d]	Singlemode FX, ST, 100 Mbit/s
		E2	EE [d][e]	Singlemode+ FX, DSC, 100 Mbit/s
		L2	LL [d]	Singlemode Longhaul, DSC, 100 Mbit/s
		G2	GG [d]	Singlemode Longhaul FX DSC 200 km, 100 Mbit/s
		O6	OO [b][f]	SFP slot, 1000 Mbit/s
		Z6	ZZ [b][f]	SFP slot, 100 Mbit/s
12 and 13 [a]	See items 10 and 11			
14	Temperature range	S		Standard 0 °C to +60 °C
		T		Extended -40 °C to +70 °C [g]
		E		Extended -40 °C to +70 °C, conformal coating [f]
15	Voltage range incl. maximum	D [h]		9.6 V DC to 60 V DC or 18 V AC to 30 V AC
	tolerances	P [i]		47 V DC to 52 V DC (PoE)
16	Certification	A		CE, UL 508, ISA 12.12.01 (UL 1604)
		H		CE, UL 508, ISA 12.12.01 (UL 1604), GL, Railway (along track), Sub Station
		B [j]		CE, UL 508, ISA 12.12.01 (UL 1604), GL, Railway (along track), Sub Station, Hazardous Location (ATEX)
17	Software variant	E		Enhanced
		P		Professional

Table 2: Combination options of device variants RS20/RS30/RS22/RS32

a. For device variants with two uplink ports you use the “Ident.” column for items 10+11 and for items 12+13.
   For device variants with three uplink ports you use the “Ident.2” column for items 10+11 and the “Ident.” column for items 12+13.
   For device variants with four uplink ports you use the “Ident.2” column for items 10+11 and for items 12+13.
b. Not in combination with “04 * 100 Mbit/s Ethernet”.
c. The last four ports of the device have PoE (Power over Ethernet).
d. For RS20-0900..., RS20-1700..., RS20-2500...;
   RS22-0900..., RS22-1700..., RS22-2500...
e. Devices with ports with product code E2 or EE: only certification “A” available (see product code for item 16).
f. In connection with “2nd uplink port” “ZZ” and “1st uplink port” “OO”.
g. Not when using GG or G2 transceivers.
   Temperature range for PoE-capable devices (RS22-..., RS32-...): -40 °C to +50 °C
h. Not for PoE-capable devices (RS22-..., RS32-...).
i. For PoE-capable devices (RS22-..., RS32-...).
j. Without railway certification EN50155 (Train).

Examples for product name

RS20- 09 00 MM M2 S D A P		
	RS20-	Rail Switch without gigabit ports
	09	9 * 100 Mbit/s Ethernet ports
	00	0 * 1000 Mbit/s Ethernet ports
	MM	Port 1 + 2 = 2 * Multimode FX, DSC, 100 Mbit/s
	M2	Port 3 = Multimode FX, DSC, 100 Mbit/s
	S	Temperature range standard: 0 °C to +60 °C
	D	Voltage range: 9.6 V DC to 60 V DC or 18 V AC to 30 V AC
	A	Certifications: CE, UL 508, ISA 12.12.01 (UL 1604)
	P	Software variant: Professional

Table 3: Example of RS20 with 3 uplink ports: RS20-0900MMM2SDAP

RS30- 08 02 O6 T1 T D A E		
	RS30-	Rail Switch with gigabit ports
	08	8 * 100 Mbit/s Ethernet ports
	02	2 * 1000 Mbit/s Ethernet ports
	O6	Port 1 = SFP slot, 1000 Mbit/s
	T1	Port 2 = twisted pair TX, RJ45 connector, 1000 Mbit/s
	T	Temperature range extended: -40 °C to +70 °C
	D	Voltage range: 9.6 V DC to 60 V DC or 18 V AC to 30 V AC
	A	Certifications: CE, UL 508, ISA 12.12.01 (UL 1604)
	E	Software variant: Enhanced

Table 4: Example of RS30 with 2 uplink ports: RS30-0802O6T1TDAE

Additional examples of devices with 3 or 4 uplink ports:

- RS20-0900**NNM4**TDAE for RS20 with 3 uplink ports (ST)
  NN: 2 * Multimode FX, ST, 100 Mbit/s (ports 1 and 2)
  M4: 1 * Multimode FX, ST, 100 Mbit/s (port 3)

- RS30-2402**OOZZ**TDAP for RS30 with 4 uplink ports (SFP)
  OO: 2 * SFP slot, 1000 Mbit/s (ports 1 and 2)
  ZZ: 2 * SFP slot, 100 Mbit/s (ports 3 and 4)

Example of device with Power over Ethernet:

- RS32-0802**O6T1**S**P**AP for RS32 with 2 uplink ports and PoE
  O6: 1 * SFP slot, 1000 Mbit/s (port 1)
  T1: 1 * twisted pair TX, RJ45, 1000 Mbit/s (port 2)
  P: Voltage range 47 V DC to 52 V DC (PoE)

1.1.2 Combination options for RS40

The product designation of your device is made from combining the desired product characteristics in accordance with the following table. The corresponding short designation is in column 3.

Item	Characteristic	Ident.	Property
1 to 4	Product	RS40	Rail Switch with gigabit ports
5	- (hyphen)	-	
6 to 7	Number of 10/100 Mbit/s ports	00	0 * 10/100 Mbit/s Ethernet
8 and 9	Number of 1000 Mbit/s ports	09	9 * 1000 Mbit/s Ethernet
10 and 11	1st + 2nd uplink ports	CC	2 * combo port multirate (SFP slot: 100/1000 Mbit/s, alternatively twisted pair RJ45 socket: 10/100/1000 Mbit/s)
12 and 13	3rd + 4th uplink ports	CC	2 * combo port multirate (SFP slot: 100/1000 Mbit/s, alternatively twisted pair RJ45 socket: 10/100/1000 Mbit/s)
14	Temperature range	S	Standard 0 °C to +60 °C
		T	Extended -40 °C to +70 °C
		E	Extended -40 °C to +70 °C, conformal coating
15	Voltage range	D	9.6 V DC to 60 V DC or 18 V AC to 30 V AC
16	Certification	A	CE, UL 508, ISA 12.12.01 (UL 1604)
		H	CE, UL 508, GL, Railway (along track), Sub Station Pending: ISA 12.12.01 (UL 1604)
		B	CE, UL 508, GL, Railway (along track), Sub Station Pending: ISA 12.12.01 (UL 1604), Hazardous Location (ATEX)
17	Software variant	E	Enhanced
		P	Professional

Table 5: Combination options for the device variants of the RS40

Examples for product name

RS40- 00 09 CC CC E D A P	RS40-	Rail Switch with gigabit ports
	00	0 * 100 Mbit/s Ethernet ports
	09	9 * 1000 Mbit/s Ethernet ports
	CC	Ports 1 + 2 = combo port: SFP slot (100/1000 Mbit/s), alternatively: RJ45 connector (10/100/1000 Mbit/s)
	CC	Ports 3 + 4 = combo port: SFP slot (100/1000 Mbit/s), alternatively: RJ45 connector (10/100/1000 Mbit/s)
	E	Temperature range extended (-40 °C to +70 °C) with conformal coating
	D	Voltage range: 9.6 V DC to 60 V DC or 18 V AC to 30 V AC
	A	Certifications: CE, UL 508, ISA 12.12.01 (UL 1604)
	P	Software variant: Professional

Table 6: Example of RS40 with 4 uplink ports: RS40-0009CCCCEDAP

1.1.3 Number of ports and media for RS20-...

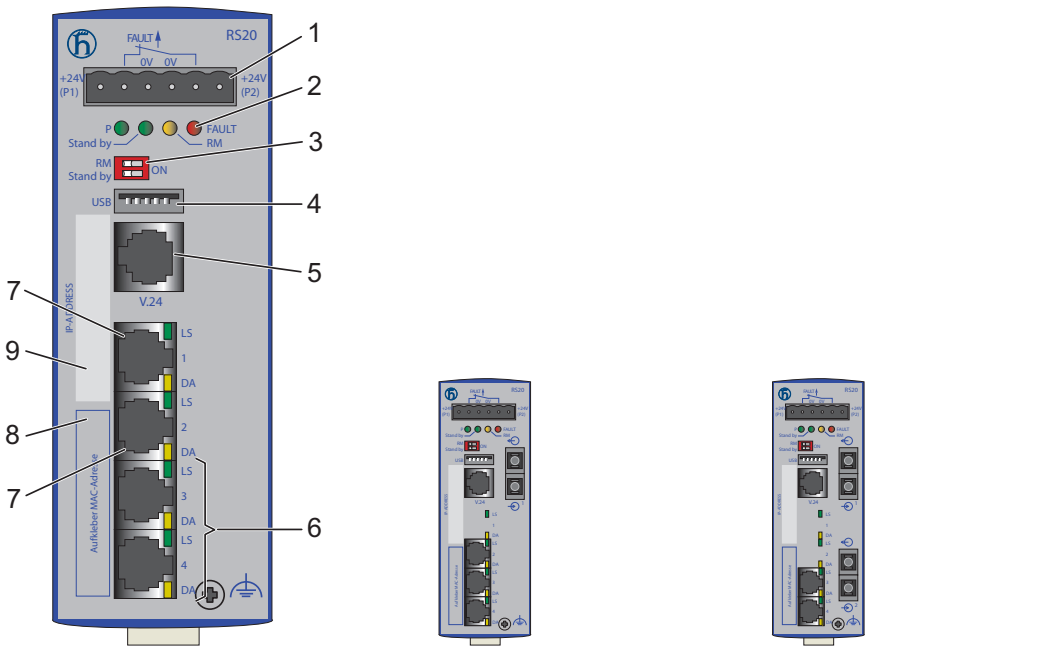


*Figure 1: Device variants with 4 * 10/100 Mbit/s ports (RS20-0400...)*
1 – plug-in terminal block, 6-pin
2 – LED display elements
3 – 2-pin DIP switch
4 – USB interface
5 – V.24 connection for external management
6 – ports in compliance with 10/100BASE-T(X) (RJ45 connections)
7 – port 1 + port 2, free choice of connections:
T1: Twisted-pair T(X), RJ45, 10/100 Mbit/s
M2: Multimode FX, DSC, 100 Mbit/s

M4: Multimode FX, ST, 100 Mbit/s
S2: Singlemode FX, DSC, 100 Mbit/s
S4: Singlemode FX, ST, 100 Mbit/s
L2: Singlemode Longhaul FX, DSC, 100 Mbit/s
G2: Singlemode Longhaul+ FX, DSC, 100 Mbit/s, 200 km

8 – MAC address field
9 – IP address field

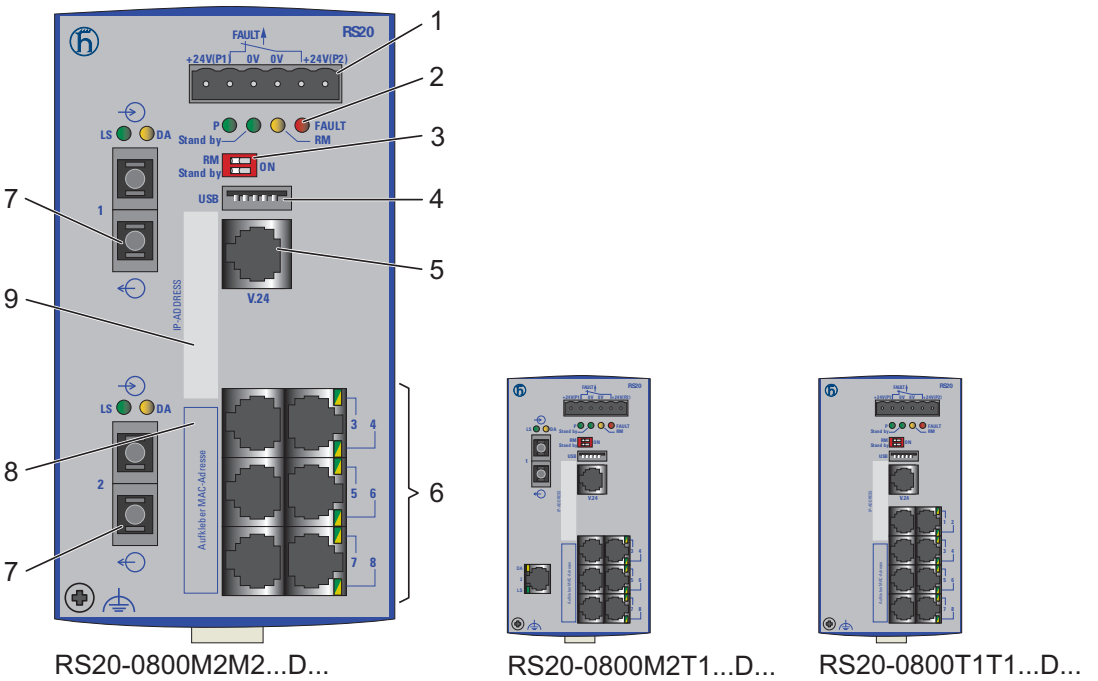


*Figure 2: Device variants with 8 * 10/100 Mbit/s ports (RS20-0800...)*
1 to 9 – see fig. 1

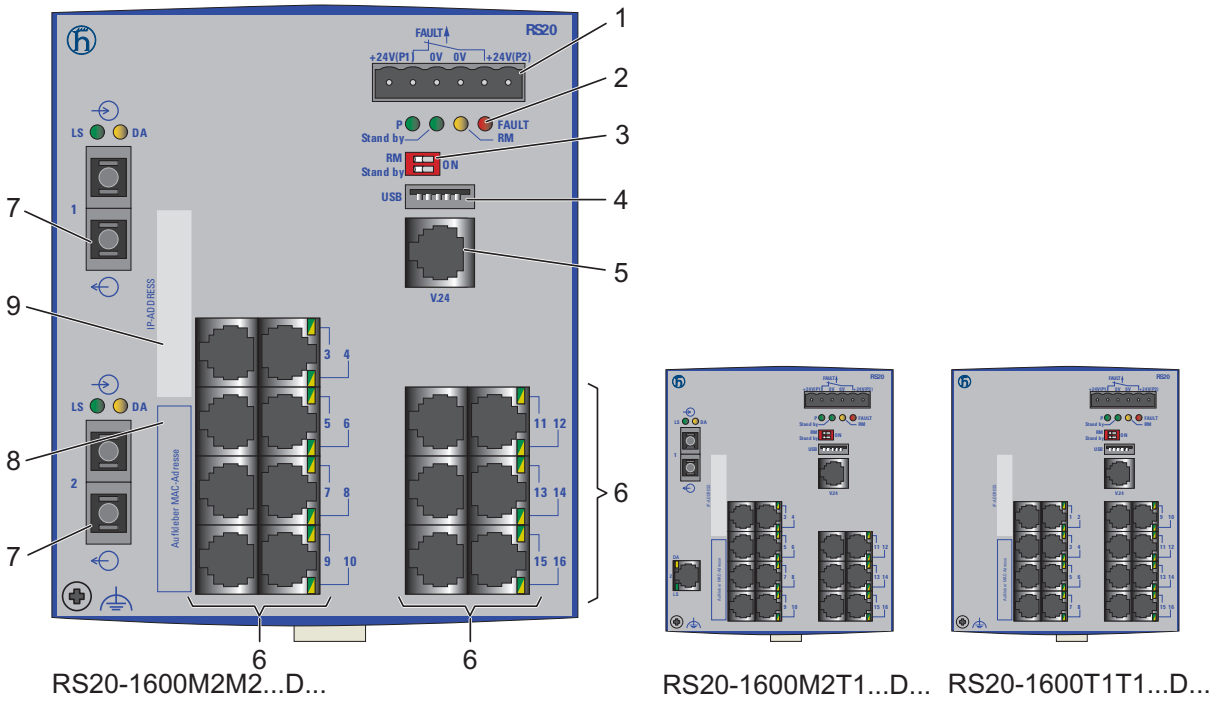


*Figure 3: Device variants with 16 * 10/100 Mbit/s ports (RS20-1600...)*
1 to 9 – see fig. 1

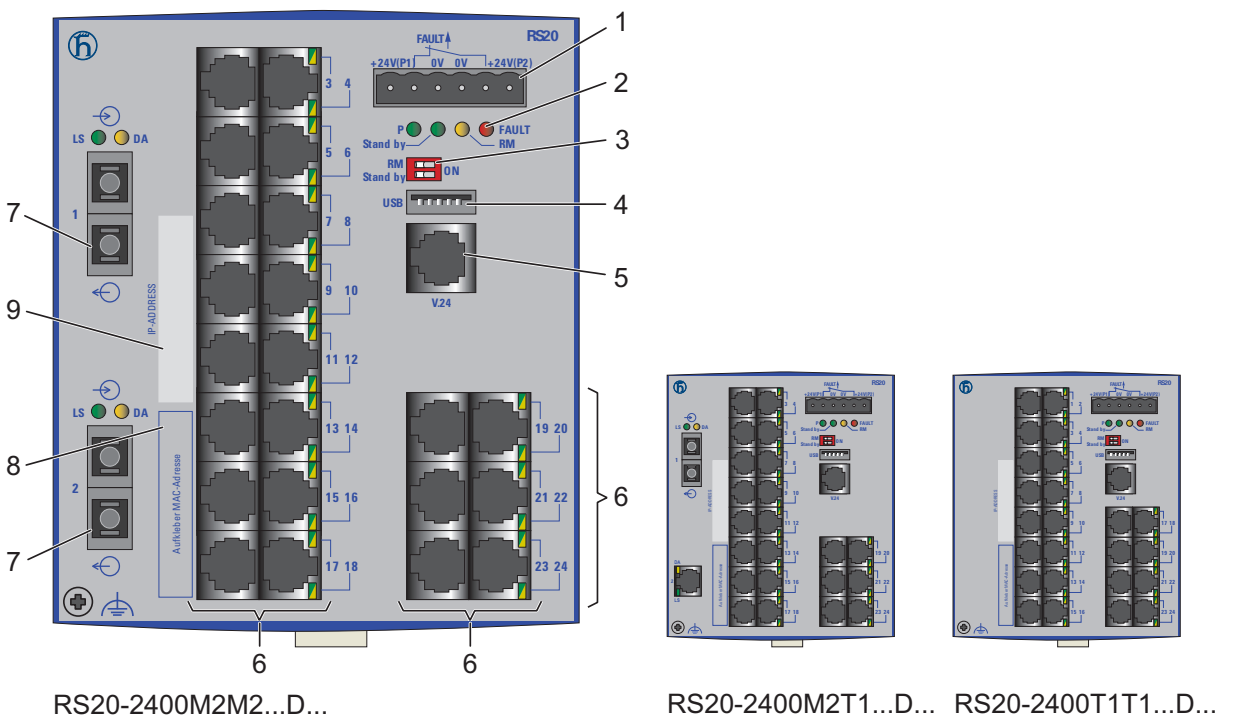


*Figure 4: Device variants with 24 * 10/100 Mbit/s ports (RS20-2400...)*
1 to 9 – see fig. 1

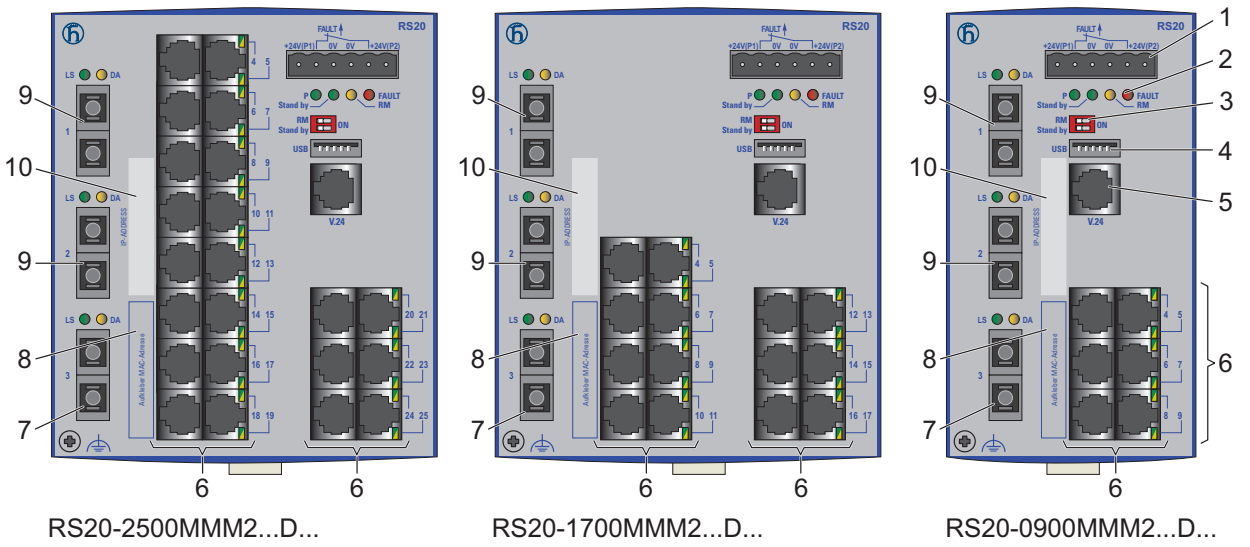


Figure 5: Device variants with 3 uplink ports (100 Mbit/s)

1 to 6 – see fig. 1

7 – port 3, free choice of connection:

T1: Twisted-pair T(X), RJ45, 10/100 Mbit/s

M2: Multimode FX, DSC, 100 Mbit/s

M4: Multimode FX, ST, 100 Mbit/s

S2: Singlemode FX, DSC, 100 Mbit/s

S4: Singlemode FX, ST, 100 Mbit/s

L2: Singlemode Longhaul FX, DSC, 100 Mbit/s

G2: Singlemode Longhaul+ FX, DSC, 100 Mbit/s, 200 km

8 – MAC address field

9 – port 1 + port 2, free choice of connections:

MM: Multimode FX, DSC, 100 Mbit/s

NN: Multimode FX, ST, 100 Mbit/s

VV: Singlemode FX, DSC, 100 Mbit/s

UU: Singlemode FX, ST, 100 Mbit/s

LL: Singlemode Longhaul FX, DSC, 100 Mbit/s

GG: Singlemode Longhaul+ FX, DSC, 100 Mbit/s, 200 km

10 – IP address field

1.1.4 Number of ports and media for RS30-...

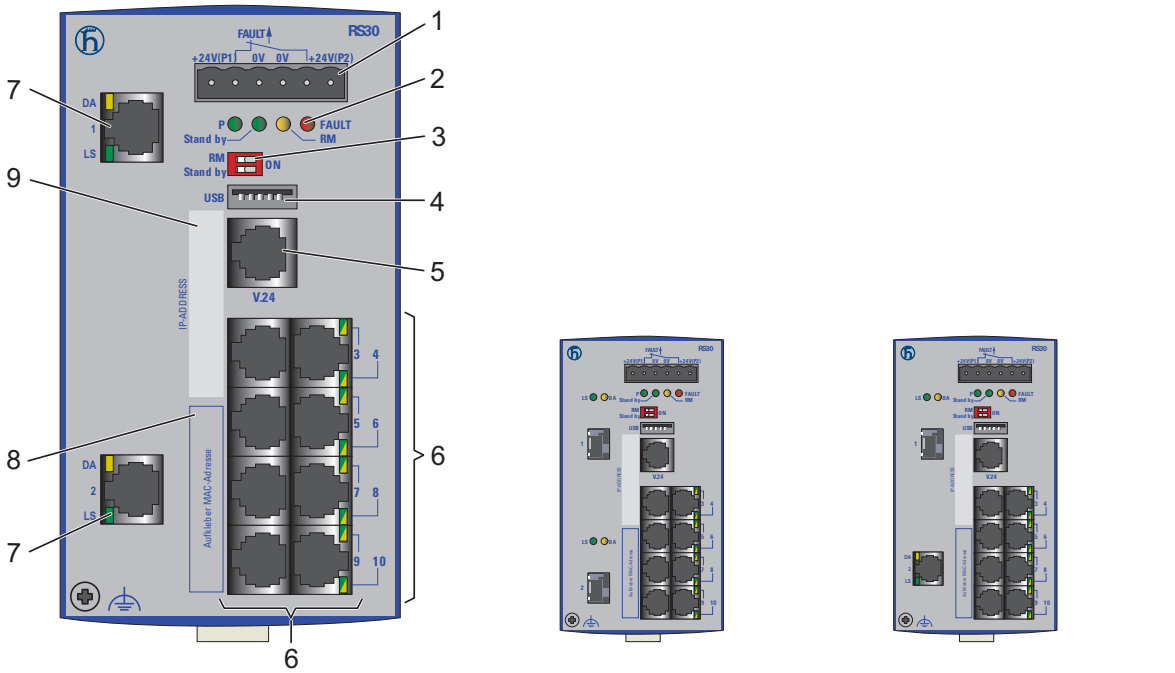


*Figure 6: Device variants with 2 * 1000 Mbit/s ports and 8 * 10/100 Mbit/s ports (RS30-0802...)*

1 – plug-in terminal block, 6-pin
2 – LED display elements
3 – 2-pin DIP switch
4 – USB interface
5 – V.24 connection for external management
6 – ports in compliance with 10/100BASE-T(X) (RJ45 connections)
7 – port 1 + port 2, free choice of connections:
T1: Twisted-pair T(X), RJ45, 10/100/1000 Mbit/s
O6: SX/LX, SFP slot, 1000 Mbit/s
8 – MAC address field
9 – IP address field

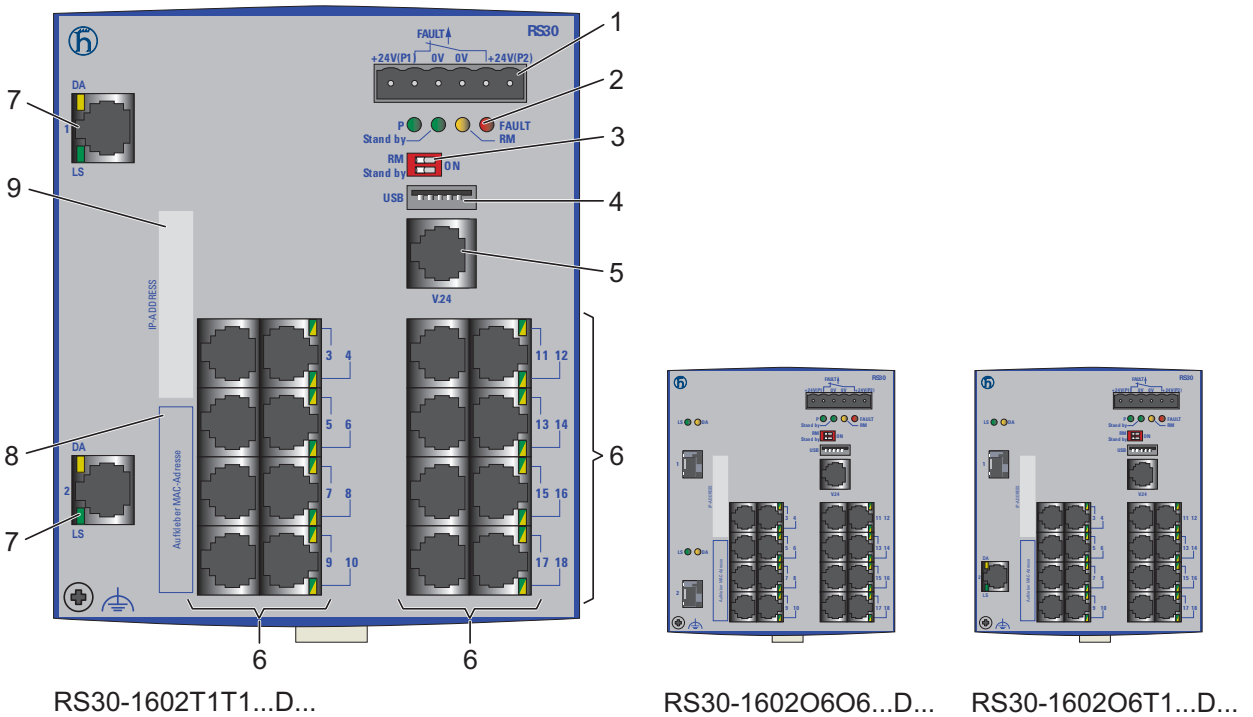


*Figure 7: Device variants with 2 * 1000 Mbit/s ports and 16 * 10/100 Mbit/s ports (RS30-1602...)*
1 to 9 – see fig. 6

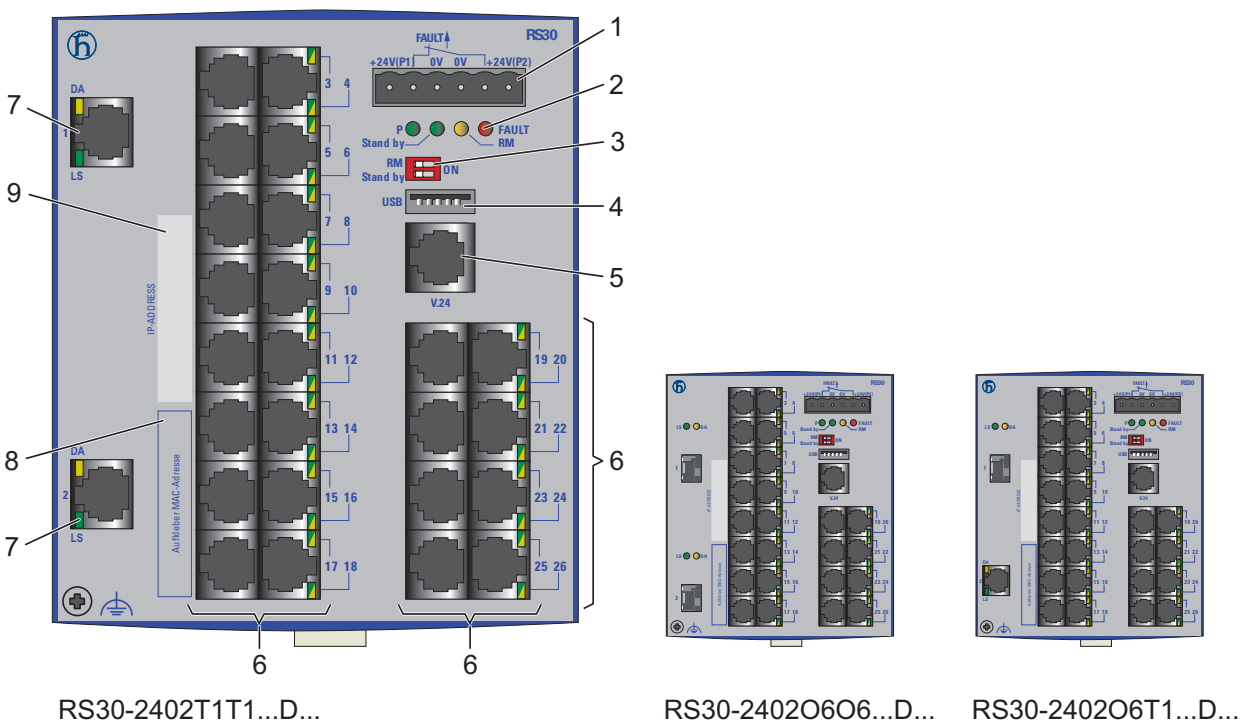


*Figure 8: Device variants with 2 * 1000 Mbit/s ports and 24 * 10/100 Mbit/s ports (RS30-2402...)*
1 to 9 – see fig. 6

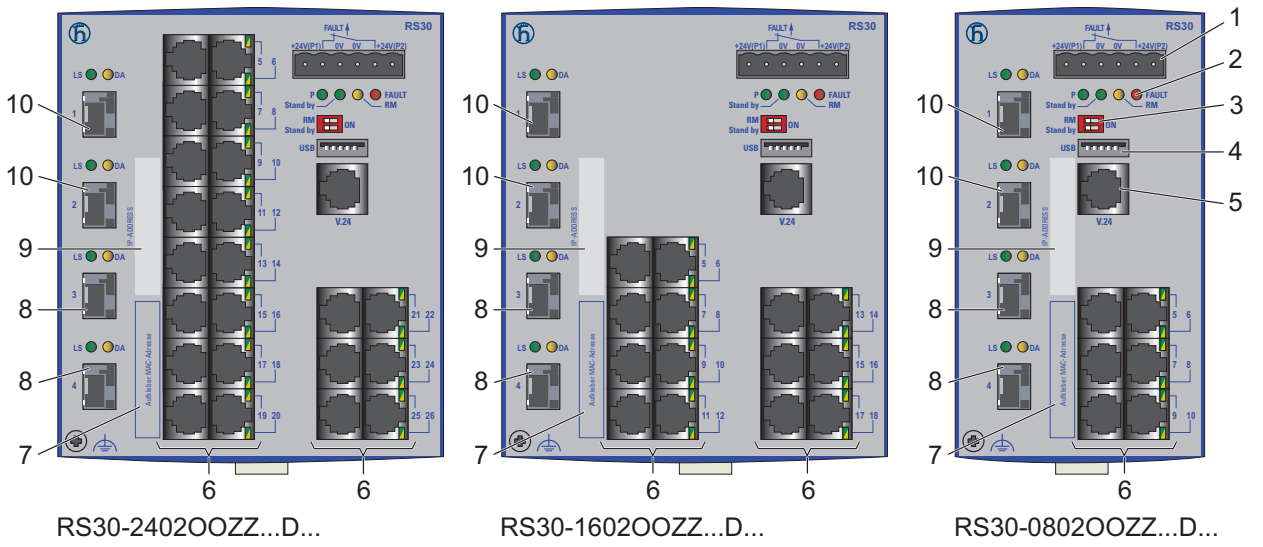
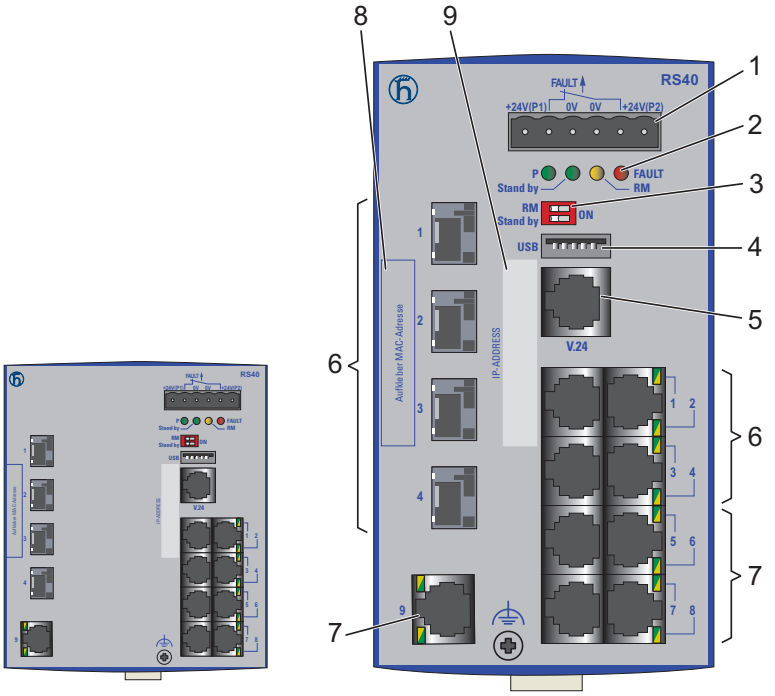


Figure 9: Device variants with 4 uplink ports
1 to 6 – see fig. 6
7 – MAC address field
8 – port 3 + port 4:
ZZ: FX, SFP slot, 100 Mbit/s
9 – IP address field
10 – port 1 + port 2:
OO: FX/SX/LX, SFP slot, 100/1000 Mbit/s

1.1.5 Number of ports and media for RS40-...



RS40-0009CCCCED...
RS40-0009CCCCTD...

RS40-0009CCCCSD...

*Figure 10: Device variants with 9 * 1000 Mbit/s ports (RS40-0009...)*

1 to 5 and 8 to 9 – see fig. 6

6 – port 1 to port 4: combo ports (CC):
FX/SX/LX, SFP slot, 100 or 1000 Mbit/s
alternatively: T(X), RJ45 connections, 10/100/1000 Mbit/s

7 – ports in compliance with 10/100/1000BASE-T(X) (RJ45 connections)

1.2 Device variants with PoE (optional)

1.2.1 Number of ports and media for devices with PoE

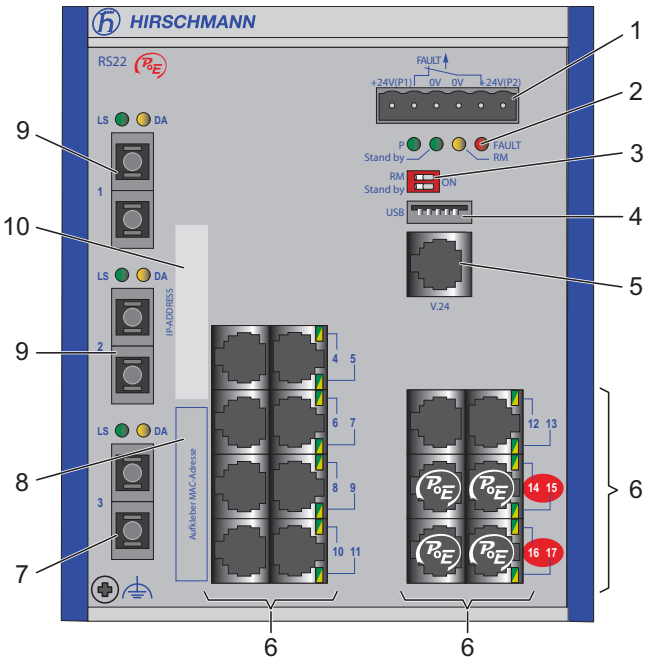


Figure 11: RS22 device variants with PoE (example: RS22-1700MMM2...P...)
1 to 5 and 7 to 9 – see fig. 5
6 – ports in compliance with 10/100BASE-T(X) (RJ45 connections; the PoE-capable ports 14 to 17 are indicated accordingly)

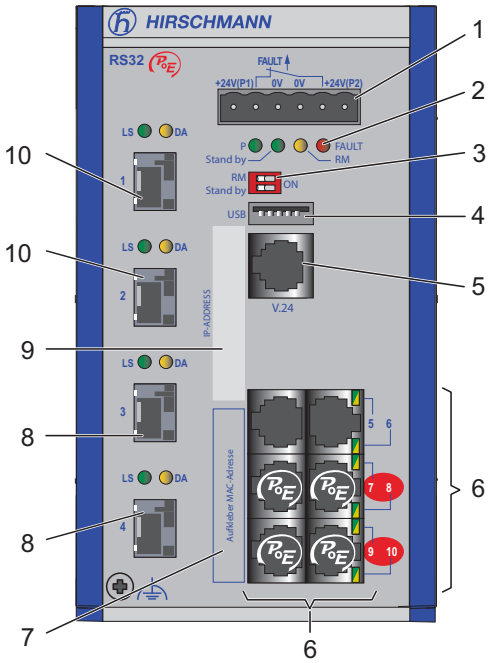


Figure 12: RS32 device variants with 4 uplink ports (example: RS32-0802OOZZ...P...)
1 to 5 and 7 to 9 – see fig. 9
6 – ports in compliance with 10/100BASE-T(X) (RJ45 connections; the PoE-capable ports 7 to 10 are indicated accordingly)

Device variants RS22-... and RS32-... support Power over Ethernet (PoE) in accordance with IEEE 802.3af.

They allow the connection and remote supply of, for example, IP telephones (Voice over IP), webcams, sensors, printer servers and WLAN access points via 10BASE-T/100BASE-TX. With PoE, these terminal devices are powered by the twisted-pair cable.

The RS22-... and RS32-... devices provide four 10BASE-T/100BASE-TX ports (RJ45 sockets) for connecting network segments or PoE terminal devices (PD, Powered Device) for all IEEE802.3af classes up to a maximum power output of 15.4 W.

The 4 PoE-capable ports are the 4 bottom ports on the right side of the device (see on page 28 ”Number of ports and media for devices with PoE“). On the device, the PoE ports are highlighted in red.
The current is supplied on wire pairs transmitting the signal; the individual ports are not electrically insulated from each other.
The following conditions are met in accordance with IEEE 802.3af:

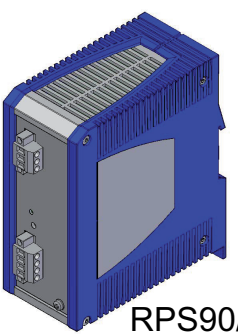
- Endpoint PSE
- Alternative A

1.2.2 PoE power units

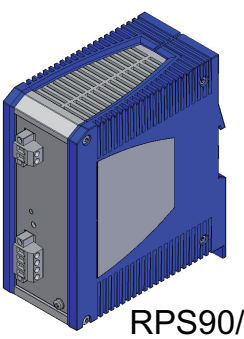
The following PoE power units are available for supplying the devices with PoE voltage:

- **RPS90/48V LV**: Low-voltage PoE power unit
  - Input voltage range: 24 V DC to 48 V DC
  - Power output at up to +60 °C: 90 W
    Power output at +60 °C to +70 °C: 60 W
- **RPS90/48V HV**: High-voltage PoE power unit
  - Input voltage range:
    60 V DC to 250 V DC or 110 V AC to 230 V AC
    You can choose between a DC or AC voltage connection.
  - Power output at up to +60 °C: 90 W
    Power output at +60 °C to +70 °C: 60 W

The output voltage can be set in the range from 48 V DC to 54 V DC.
The default setting for the output voltage is 48 V DC.



RPS90/48V HV



RPS90/48V LV

2 Assembly and start-up

The devices have been developed for practical application in a harsh industrial environment. The installation process is correspondingly simple. On delivery, the device is ready for operation.

The following steps should be performed to install and configure a switch:

- Unpacking and checking
- Installing the SFP modules (optional)
- Insert data in label area
- Adjust DIP switch settings
- Connect PoE power unit (optional)
- Connect the terminal block for voltage supply and signal contact and connect the supply voltage
- Install the device on the DIN rail, grounding
- Install the terminal block, start-up procedure
- Connecting the data lines

2.1 Installing the device

2.1.1 Unpacking and checking

☐ Check that the contents of the package are complete (see page 59 ”Scope of delivery“).
☐ Check the individual parts for transport damage.

2.1.2 Installing the SFP modules (optional)

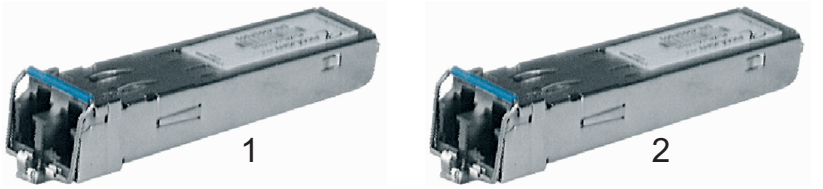


Figure 13: 1 - Fast EHTERNET fiber optic SFP module
2 - Gigabit ETHERNET fiber optic SFP module

☐ Before attaching an SFP module, first remove the protective cap over the socket.
☐ Push the SFP module with the lock closed into the socket until it latches audibly in place.

Note: Only use Hirschmann SFP modules (see page 60 ”Accessories“).

2.1.3 Insert data in label area

The information field for the IP address on the front of the device helps you to structure your network installation clearly.

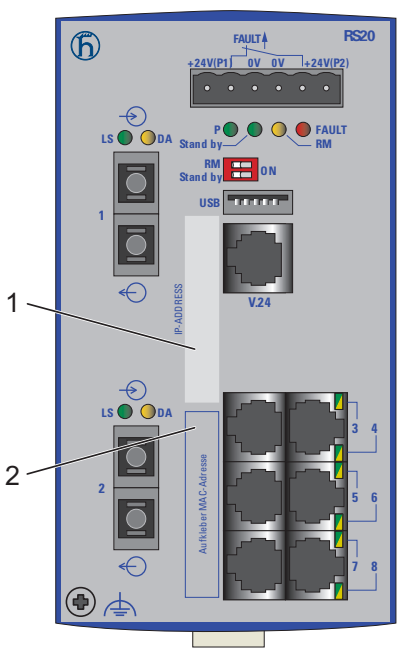


Figure 14: Label area for IP address of device
1 – IP address of device (label area)
2 – MAC address of device (label)

2.1.4 Adjust DIP switch settings

The 2-pin DIP switch on the front panel of the device gives you the following options:

Figure 15: 2-pin DIP switch

Switch RM position	Switch stand-by position	Ring redun-dancy	Coup-ling switch	Ring Manag er	Coupli ng Manag er	Ring port	Control port	Coup ling port	Software configuration
OFF	OFF	on	on	off	off	1 + 2			
ON	OFF	on	on	on	off	1 + 2			
OFF	ON	on	on	off	on	1 + 2	3	4	
ON	ON								SW config. has priority over DIP switch configuration

State on delivery: both DIP switches “ON”.

☐ Before starting operation of the device, check whether the default settings of the DIP switch correspond to your requirements.

2.1.5 RS20/RS30/RS40: supply voltage and signal contact

The supply voltage and the signal contact are connected via a 6-pin terminal block with a snap lock.

Caution!
Note the safety instructions (see page 4 ”Notes on safety“) and only connect a supply voltage that corresponds to the type plate of your device. Make sure that the contact load capability of the signal contact is not exceeded (see page 53 ”Technical data“).

Supply voltage for RS20/RS30/RS40

Redundant power supplies can be used. Both inputs are uncoupled. There is no distributed load. With redundant supply, the power supply unit supplies the device only with the higher output voltage. The supply voltage is electrically isolated from the housing.
See “Insulation voltage” in chapter ”Technical data“ on page 53.

You can choose between DC or AC voltage when connecting the supply voltage. You use the +24V and 0V pins to connect the AC voltage (see fig. 16).

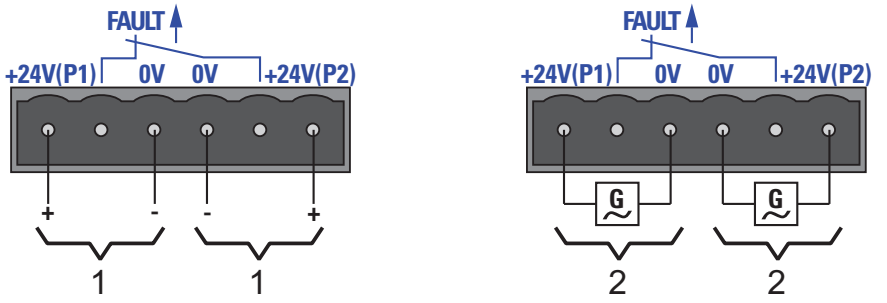


Figure 16: Connecting the supply voltage at the 6-pin terminal block
1 – DC voltage, voltage range: 9.6 V DC to 60 V DC
2 – AC voltage, voltage range: 18 V AC to 30 V AC

Note: With non-redundant supply of the main voltage, the device reports a loss of power. You can avert this message by applying the supply voltage via both inputs, or by changing the configuration in the Management.

Signal contact for RS20/RS30/RS40

- The signal contact (“FAULT”, for pin assignment of terminal block, see fig. 16) monitors the functioning of the device, thus enabling remote diagnostics. You can specify the type of function monitoring in the Management.
- You can also use the switch Web page to switch the signal contact manually and thus control external devices.

A break in contact is used to report the following conditions via the potential-free signal contact (relay contact, closed circuit):

- The detected inoperability of at least one of the two voltage supplies (voltage supply 1 or 2 is below the threshold value).
- A continuous malfunction in the device.
- The loss of connection at at least one port. The report of the link status can be masked by the Management for each port. In the delivery state, link status monitoring is deactivated.
- The loss of ring redundancy reserve.
- A detected error during the self-test.
- Incorrect configuration of the HIPER-Ring or ring coupling.

The following condition is also reported in RM mode:

- Ring redundancy reserve is available. On delivery, there is no ring redundancy monitoring.

☐ Pull the terminal block off the device and connect the power supply and signal lines.

2.1.6 RS22/RS32: supply voltage and signal contact

For the RS22/RS32, the PoE supply voltage and the signal contact are connected via the 6-pin terminal block with a snap lock.

The RS22/RS32 devices are supplied with PoE voltage (48 V DC safety low voltage) via an external power supply unit.

☐ Make sure that the external power supply unit you use to provide the PoE voltage fulfills the following basic prerequisites:
- Insulation requirements according to IEEE 802.3af (insulation resistance 48 V, output to “rest of the world” 2,250 V DC for 1 min.).
- Output power < 100 W
- Current limitation < 5 A
- The power supply unit and the devices with PoE ports form a “limited power source” according to IEC 60950-1.
- The external PoE power supply unit must be able to provide the power for the connected PDs (Power Devices) and for the Switch.

Note: The RS22/RS32 devices fulfill the technical data and the certifications when using the RPS90/48V LV and RPS90/48V HV power units from Hirschmann. Only use these power units, to ensure that the specifications are fulfilled.

RPS90/48V LV: connecting the input voltage

With the RPS90/48V LV low-voltage PoE power unit, you connect a DC supply voltage of 24 V DC to 48 V DC at the input connection.

The supply voltage is connected via pin 1 and pin 2.

Figure	Pin	Assignment	Voltage range
	1	Minus terminal of the supply voltage	Low voltage input voltage: 24 V DC to 48 V DC
	2	Plus terminal of the supply voltage	

Table 7: Connecting the low-voltage supply voltage at PoE power unit RPS90/48V LV

☐ First connect the protective conductor to the protective conductor terminal.
☐ Connect the DC voltage to the 2-pin terminal block.
☐ Use a supply cable with a maximum length of 2 meters to the power unit.

RPS90/48V HV: connecting the input voltage

With the RPS90/48V HV high-voltage PoE power unit, you connect either a DC or AC supply voltage at the input connection:
- 60 V DC to 250 V DC
- 110 V AC to 230 V AC

The supply voltage is connected via pin 2 and pin 3, and the protective conductor is connected via pin 1.

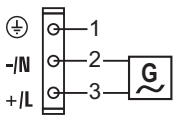
Figure	Pin	Assignment	Voltage range
	1	Protective conductor	High voltage input voltage: 110 V AC to 230 V AC
	2	Minus terminal of the supply voltage	
	3	Plus terminal of the supply voltage	

Table 8: Connecting the high-voltage supply voltage at PoE power unit RPS90/ 48V HV (AC voltage)

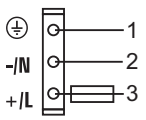
Figure	Pin	Assignment	Voltage range
	1	Protective conductor	High-voltage input voltage: 60 V DC to 250 V DC
	2	Minus terminal of the supply voltage	
	3	Plus terminal of the supply voltage	
		= external fuse for supply voltages > 125 V DC	

Table 9: Connecting the high-voltage supply voltage at PoE power unit RPS90/ 48V HV (DC voltage)

- ☐ First connect the protective conductor to the protective conductor terminal.
- ☐ Connect the supply voltage via the 3-pin terminal block. Pay attention to the +/L and -/N connections.
- ☐ If the neutral conductor or the minus terminal of the supply voltage is not grounded, install a suitable fuse in the input line.
- ☐ For supply voltages > 125 VDC:
  Install a suitable external fuse in the supply voltage input line of the plus terminal.
- ☐ Use a supply cable with a maximum length of 2 meters to the power unit.

RS22/RS32 supply voltage

The RPS90/48V LV and RPS90/48V HV PoE power supply units provide an output voltage of typically 48 V DC for supplying the RS22-.../RS32-... devices with the PoE voltage.

Caution!
Note the safety instructions (see page 4 ”Notes on safety“) and only connect a supply voltage that corresponds to the type plate of your device. Make sure that the contact load capability of the signal contact is not exceeded (see page 53 ”Technical data“).

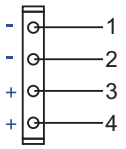
Figure	Pin	Assignment	Voltage range
	1+2	Minus terminal of the output voltage	Output voltage (PoE voltage) range: 48 V DC to 54 V DC (default: 48 V DC)
	3+4	Plus terminal of the output voltage	

Table 10: Output voltage of RPS90/48V LV and RPS90/48V HV PoE power units

☐ Connect the PoE voltage to the 6-pin terminal block for the device included in the delivery.
Make sure the following requirements are met:
- Supply line length < 0.5 m.

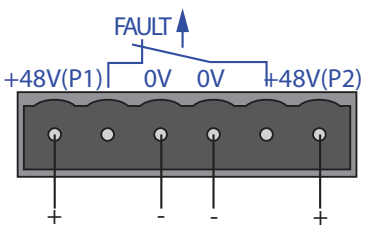


Figure 17: Connecting the PoE supply voltage at the 6-pin terminal block of device RS22/RS32

RS22/RS32 signal contact

- The signal contact (“FAULT”, for pin assignment of terminal block, see fig. 17) monitors the functioning of the device, thus enabling remote diagnostics. You can specify the type of function monitoring in the Management.
- You can also use the switch Web page to switch the signal contact manually and thus control external devices.

A break in contact is used to report the following conditions via the potential-free signal contact (relay contact, closed circuit):

- The detected inoperability of at least one of the two voltage supplies (voltage supply 1 or 2 is below the threshold value).
- A continuous malfunction in the device.
- The loss of connection at at least one port. The report of the link status can be masked by the Management for each port. In the delivery state, link status monitoring is deactivated.
- The loss of ring redundancy reserve.
- A detected error during the self-test.
- Incorrect configuration of the HIPER-Ring or ring coupling.

The following condition is also reported in RM mode:
- Ring redundancy reserve is available. On delivery, there is no ring redundancy monitoring.

☐ Pull the terminal block off the device and connect the power supply and signal lines.

2.1.7 Installing the device on the DIN rail, grounding

Mounting on the DIN rail

The devices are mounted very quickly by snapping them onto the DIN rail.

☐ Mount the device on a 35 mm DIN rail in accordance with DIN EN 60175.

☐ Attach the upper snap-in guide of the device into the DIN rail and press it down against the DIN rail until it snaps into place.

Note: The shielding ground of the connectable twisted pair lines is connected to the front panel as a conductor.

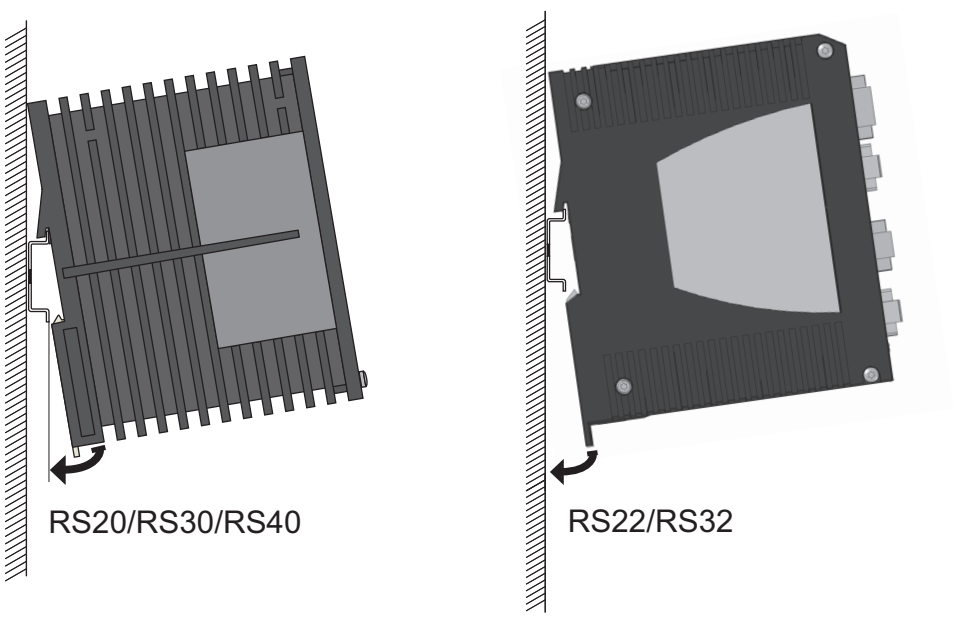


Figure 18: Mounting on the DIN rail

DIN rail mounting on ships (RS30-0802...)

When you are mounting your RS30-0802... Open Rail device on a DIN rail on ships and in similar applications, the Open Rail Mounting Kit available as an accessory can be used to avoid excessive resonance.

☐ You must use the Open Rail Mounting Kit with the order number 942 007-001 (see page 60 ”Accessories“) when mounting your RS30-0802... device on ships.
If you have very little space on your DIN rail, you can alternatively use Open Rail Mounting Kit 942 007-101 (for mounting DIN rail on DIN rail).

☐ Mount one mounting kit on each side of your RS30-0802... device, but at least one mounting kit on one side of the RS30-0802... device. If possible, position one side of the RS30-0802... device on a wall, or in a similarly stable way. If you are positioning multiple RS30-0802... devices side by side, mount the row of devices in the way described for a single device.

☐ Mount a standard DIN rail stopper on both sides beside the mounting kit.

For more information on mounting the RS30-0802... on a DIN rail on ships, see the “Open Rail Mounting Kit Mounting Instructions” manual supplied with the Open Rail Mounting Kit.

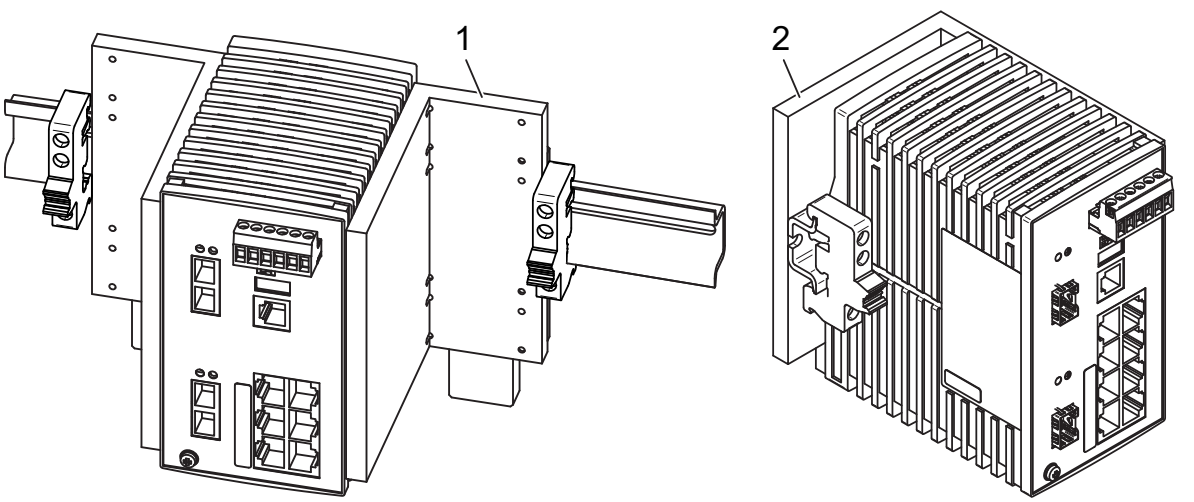


Figure 19: Mounting the RS30-0802... on ships with the Open Rail Mounting Kit
1 - Open Rail Mounting Kit 942 007-001
2 - Open Rail Mounting Kit 942 007-101

Mounting on the wall (RS22/RS32)

In addition to the option of mounting them on a DIN rail, you can also mount the RS22/RS32 devices on the wall using the wall mounting plate supplied (see page 60 ”Accessories“).

Figure 20: Mounting the RS22/RS32 devices on the wall

☐ Mount the device on the wall plate as shown in the illustration. Insert the upper snap-in guide of the device into the rail and press it down against the rail until it snaps into place.

☐ Fasten the wall plate (see on page 60 ”Accessories“) on a level wall surface using four screws.

Grounding

With the RS20/RS30/RS40, the front panel of the device is grounded via the separate ground screw.
With the RS22/RS32, the front panel and the metal housing of the device is grounded via the separate ground screw.

☐ For the ground conductor, use a cable with a cross section of at least 1.0 mm².

2.1.8 Dimension drawings

Dimension drawings for RS20/RS30/RS40

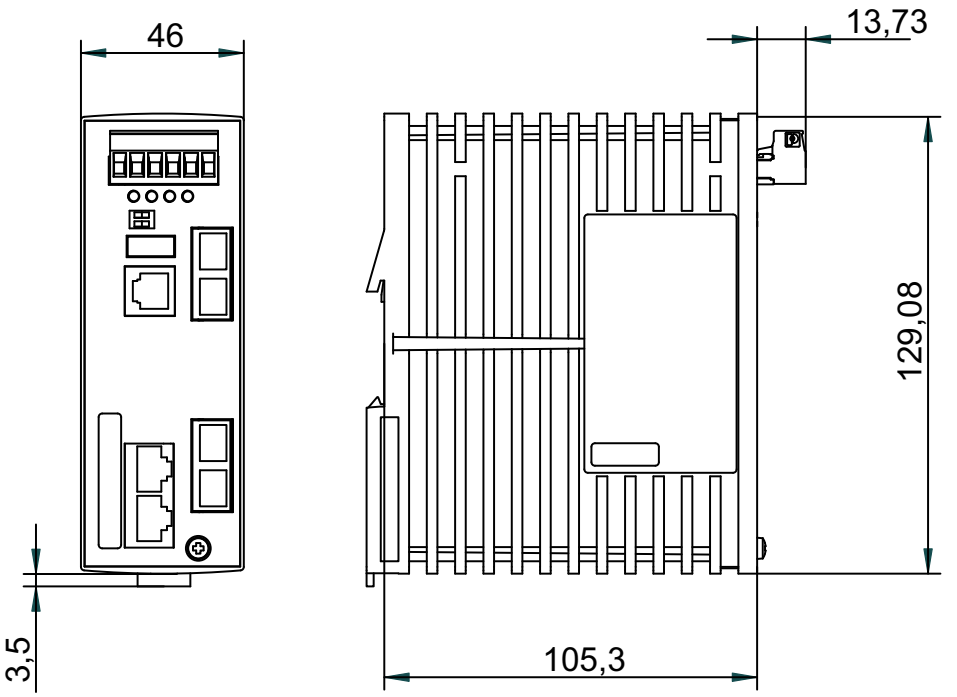


Figure 21: Dimensions of device variants RS20-04... with 4 ports

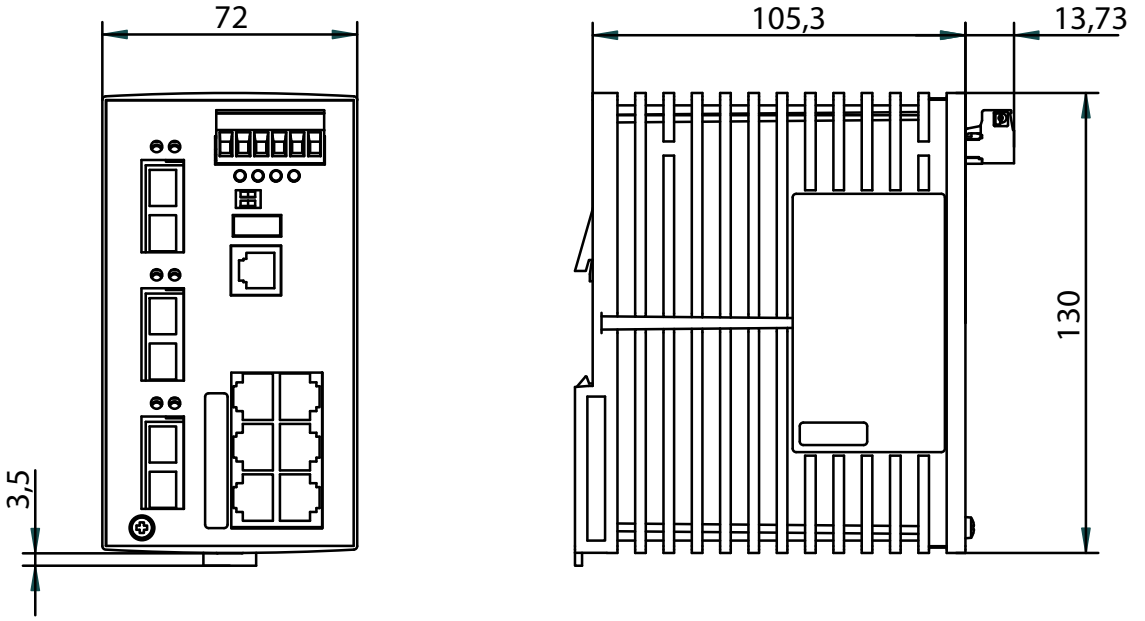


Figure 22: Dimensions of device variants RS20.../RS30.../RS40... with 8 to max. 10 ports

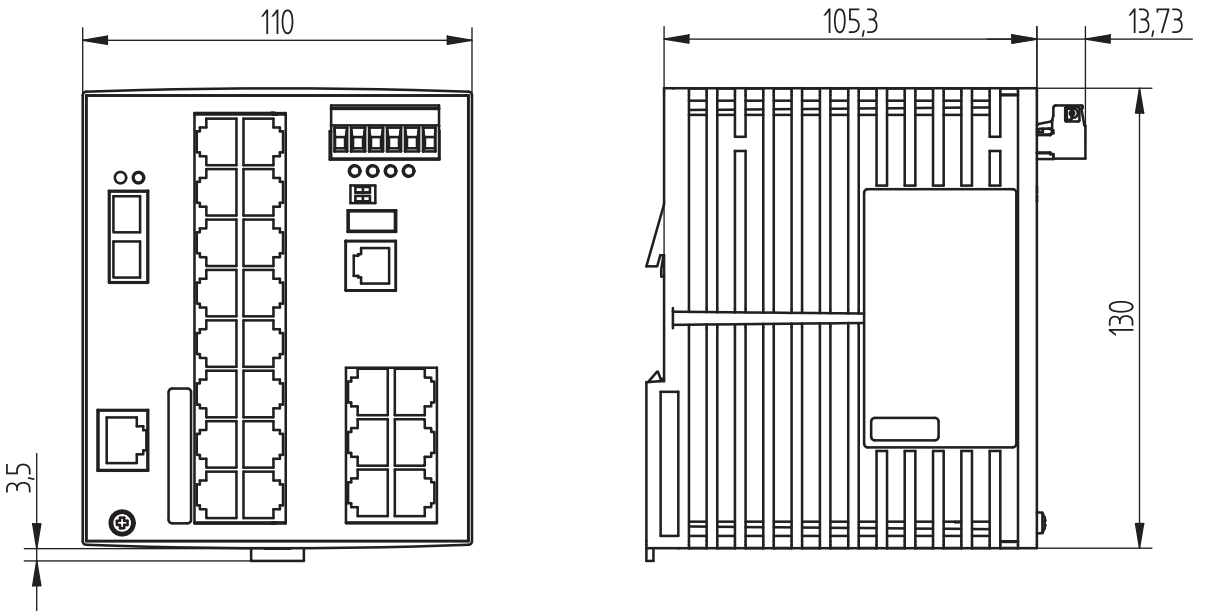


Figure 23: Dimensions of device variants RS20.../RS30.../RS40... with 16 to max. 26 ports

Dimension drawings for RS22/RS32

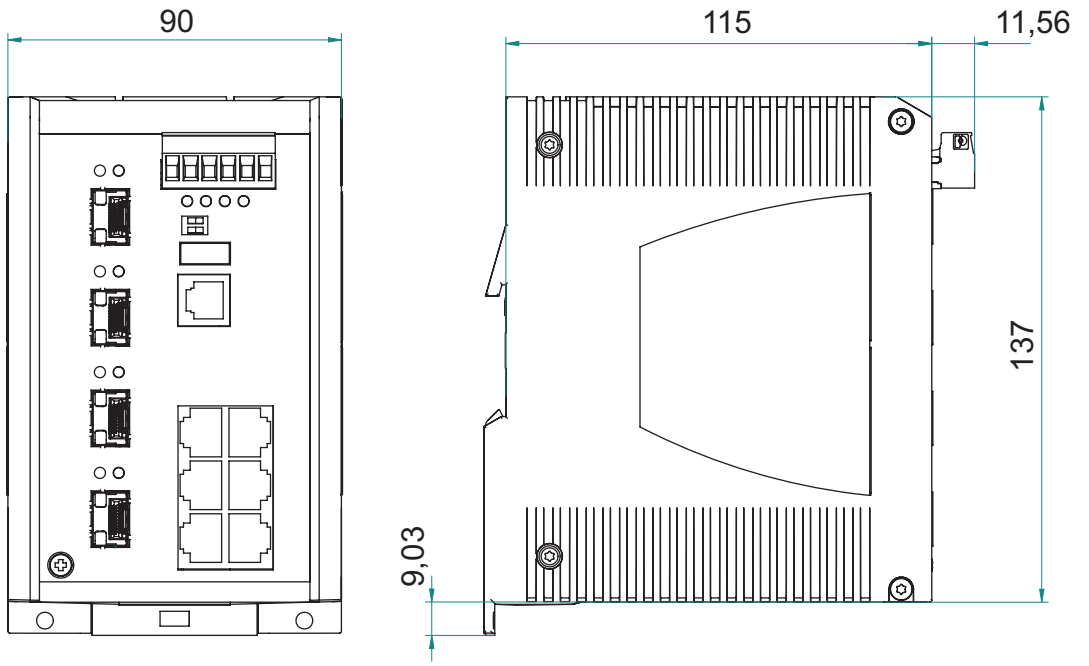


Figure 24: Dimensions of device variants RS22.../RS32... with 8 to max. 10 ports

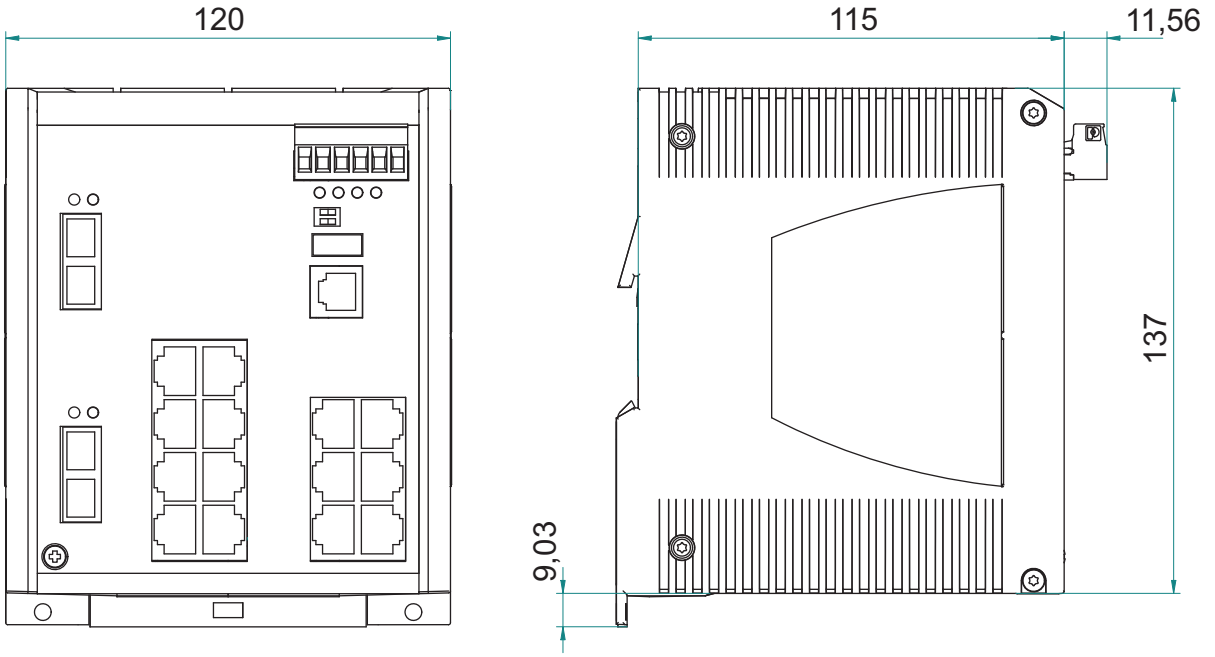


Figure 25: Dimensions of device variants RS22.../RS32... with 16 to max. 26 ports

Dimension drawings for PoE power units

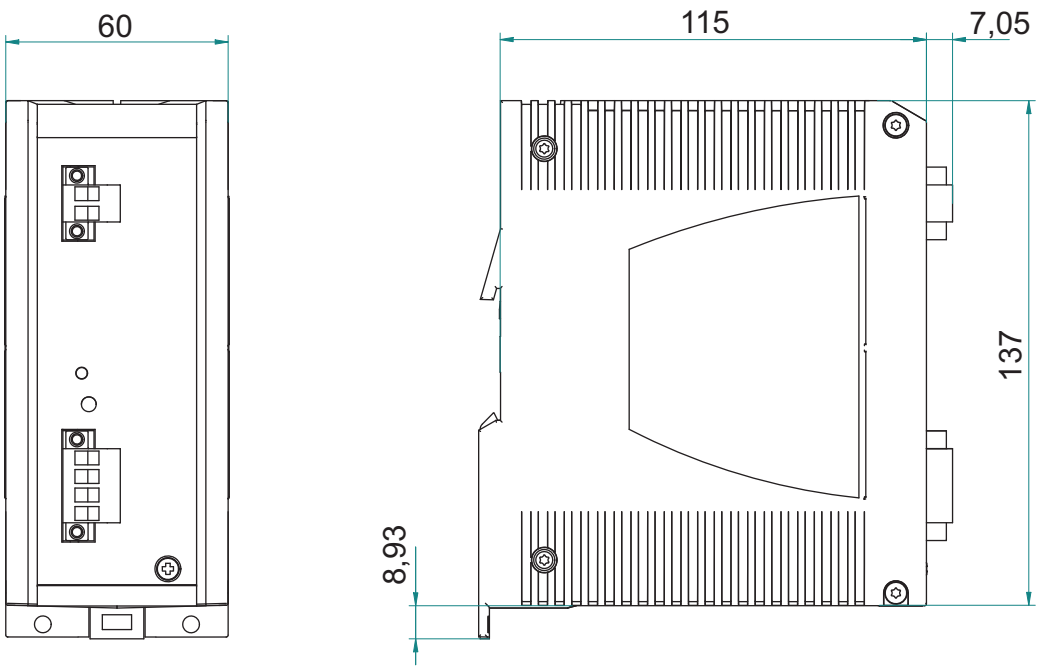


Figure 26: Dimensions of RPS90/48V LV and RPS90/48V HV PoE power units

2.1.9 Connecting the ferrite

Note: For PoE devices with 16 or more ports (RS22-16..., RS22-17..., RS22-24... and RS22-25...):

To adhere to EMC conformity, you connect the ferrite supplied to the 48V output of the voltage supply line (see fig. 27).

☐ Insert both cables of the 48V output through the ferrite twice.
☐ Lock the ferrite.
☐ The ferrite should be connected as close as possible to the output (max. distance 50 cm).

The ferrite can be opened with the key supplied.

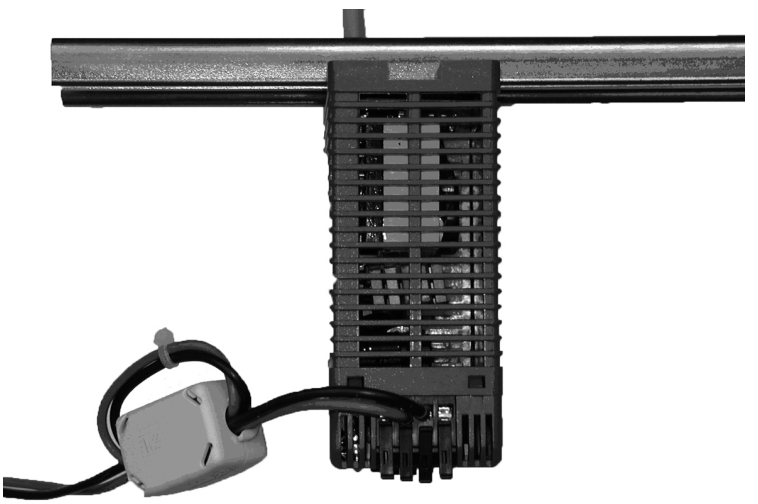


Figure 27: Connecting the ferrite to the voltage supply line

2.1.10 Installing the terminal block, start-up procedure

☐ Mount the terminal block for the voltage supply and signal contact on the front of the device using the snap lock. Make sure that the snap lock snaps into place.

Connecting the voltage supply via the terminal block starts the operation of the device.

2.1.11 Connecting the data lines

You can connect terminal devices and other segments at the ports of the device via twisted pair cables or F/O cables.

☐ Install the data lines according to your requirements.

■ **10/100 Mbit/s twisted pair connection**
These connections are RJ45 sockets.

10/100 Mbit/s TP ports enable the connection of terminal devices or independent network segments according to the IEEE 802.3 10BASE-T/ 100BASE-TX standard.
These ports support:
- Autonegotiation
- Autopolarity
- Autocrossing (if autonegotiation is activated)
- 100 Mbit/s half-duplex mode, 100 Mbit/s full duplex mode
- 10 Mbit/s half-duplex mode, 10 Mbit/s full duplex mode

State on delivery: autonegotiation activated.
The socket housing is electrically connected to the front panel.

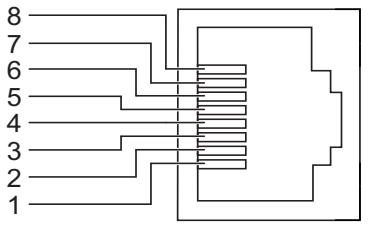
Figure	Pin	Function
	1+2	One line pair: receiver path
	3+6	One line pair: sender path
	4,5,7,8	Not used

Table 11: Pin assignment of a TP/TX interface in MDI-X mode, RJ45 socket

10/100 Mbit/s twisted-pair connection PoE (RS22-.../RS32-...)

These connections are RJ45 sockets.
10/100 Mbit/s TP PoE ports enable the connection of terminal devices or independent network segments according to the IEEE 802.3 10BASE-T/ 100BASE-TX and IEEE 802.3af (Power over ETHERNET on data lines) standards.
These ports support:
- Autonegotiation
- Autopolarity
- Autocrossing (if autonegotiation is activated)
- 100 Mbit/s half-duplex mode, 100 Mbit/s full duplex mode
- 10 Mbit/s half-duplex mode, 10 Mbit/s full duplex mode
- Power over ETHERNET (PoE, at the last four ports of the device)

State on delivery: autonegotiation activated.
The socket housing is electrically connected to the front panel.
The PoE voltage is input via the wire pairs transmitting the signal (phantom voltage).

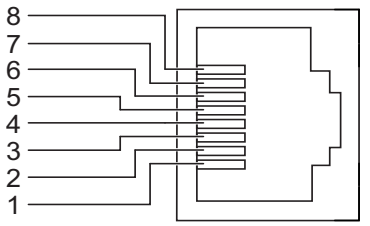
Figure	Pin	Function		PoE
	1	RD+	Receive Data +	V-
	2	RD-	Receive Data -	V-
	3	TD+	Transmit Data +	V+
	6	TD-	Transmit Data -	V+
	4,5,7,8	Not used		

Table 12: Pin assignment of a TP/TX interface for PoE for the voltage supply to the wire pairs transmitting the signal, RJ45 socket, MDI-X mode

10/100/1000 Mbit/s twisted pair connection

These connections are RJ45 sockets.

10/100/1000 Mbit/s TP ports enable the connection of terminal devices or independent network segments according to the IEEE 802.3 10BASE-T/ 100BASE-TX/1000BASE-T standard.

These ports support:

- Autonegotiation
- Autopolarity
- Autocrossing (if autonegotiation is activated)
- 1000 Mbit/s full duplex
- 100 Mbit/s half-duplex mode, 100 Mbit/s full duplex mode
- 10 Mbit/s half-duplex mode, 10 Mbit/s full duplex mode

State on delivery: autonegotiation activated.
The socket housing is electrically connected to the front panel.
The pin assignment corresponds to MDI-X.

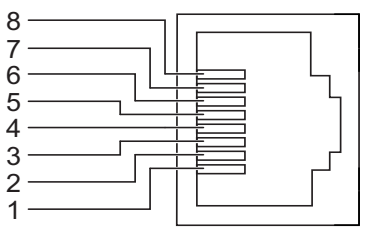
Figure	Pin	Function
	1	BI_DB +
	2	BI_DB -
	3	BI_DA +
	4	BI_DD +
	5	BI_DD -
	6	BI_DA -
	7	BI_DC +
	8	BI_DC -

Table 13: Pin assignment of a 1000 MBit/s TP interface in MDI-X mode, RJ45 socket

100 Mbit/s F/O connection

In device variants RS20 and RS22, these ports are DSC connectors or ST connectors.
In device variants RS30, RS32 and RS40, these ports are SFP slots.
100 MBit/s F/O ports enable the connection of terminal devices or independent network segments in compliance with the IEEE 802.3 100BASE-FX standard.
These ports support:

- Full or half duplex mode

State on delivery: full duplex FDX

Note: Make sure that the LH ports are only connected with LH ports, SM ports are only connected with SM ports, and MM ports only with MM ports.

1 Gbit/s F/O connection

These ports are SFP slots.
1 Gbit/s F/O ports enable the connection of terminal devices or independent network segments according to the IEEE 802.3 1000BASE-SX/1000BASE-LX standard.
These ports support:

- Autonegotiation

Note: Make sure that the LH ports are only connected with LH ports, SX ports are only connected with SX ports, and LX ports only with LX ports.

Note: In device variants RS30-...02OOZZ... and RS32-...02OOZZ... (four uplink ports with SFP slot) Gigabit-ETHERNET-SFP transceivers or Fast-ETHERNET-SFP transceivers can be mounted at the two top ports, and Fast-ETHERNET-SFP transceivers can be mounted at the two bottom ports (see page 60 ”Accessories“).
In device variants RS40-... Gigabit-ETHERNET-SFP transceiver or Fast-ETHERNET-SFP transceiver can be mounted at the combo ports (see page 60 ”Accessories“).

2.2 Display elements

After the operating voltage is set up, the software starts and initializes itself. Afterwards, the device performs a self-test. During this process, various LEDs light up. The process takes around 60 seconds.

Device state

These LEDs provide information about conditions which affect the operation of the whole device.

Figure 28: Device status LEDs

P - Power (green/yellow LED)	
Glowing green	Both supply voltages are on
Glowing yellow	There is only one supply voltage (P1 or P2) on
Not glowing	Supply voltages P1 and P2 are too low
FAULT - error, signal contact (red LED) [a]	
Glowing red	The signal contact is open, i.e. it is reporting an error.
Not glowing	The signal contact is closed, i.e. it is not reporting an error.

a. If the manual adjustment is active on the “FAULT” signal contact, then the detected error display is independent of the setting of the signal contact.

RM - Ring Manager (green/yellow LED)	
Glowing green	RM function active, redundant port disabled
Glowing yellow	RM function active, redundant port enabled
Not glowing	RM function not active
Flashing green	Incorrect configuration of the HIPER-Ring (e.g. the ring is not connected to the ring port).
Stand-by	
Glowing green	Stand-by mode enabled
Not glowing	Stand-by mode not enabled
RM and Stand-by - display saving processes of the AutoConfiguration Adapter (ACA)	
Flashing alternately	Error during saving process.
LEDs flash synchronously, two times a second	Loading configuration from the ACA.
LEDs flash synchronously, once a second	Saving the configuration in the ACA.

Port state

The green and yellow LEDs at the individual port display port-related information. During the boot phase, these LEDs are used to display the status of the boot procedure.

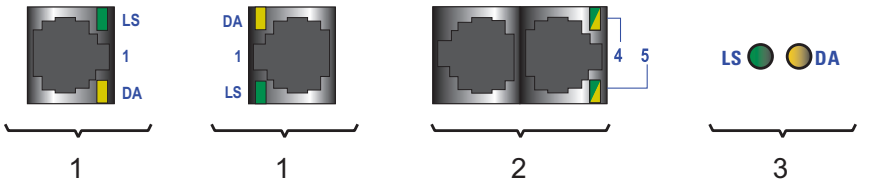


Figure 29: Port status LEDs

1 – Port status LEDs for isolated or single-row RJ45 sockets: one green and one yellow LED per port.

2 – Port status LEDs for double-row RJ45 sockets: one LED per port, glowing/flashing either green or yellow.

3 – Port status LEDs for DSC, ST, SFP

LS - link status (green LED)	
Not glowing	No valid connection.
Glowing green	Valid connection.
Flashing green (1 time a period)	Port is switched to stand-by.
Flashing green (3 times a period)	Port is switched off.
DA - data (yellow LED)	
Not glowing	No data reception at corresponding port
Flashing yellow	Data reception at corresponding port

2.3 Basic set-up

The IP parameters must be entered when the device is installed for the first time. The device provides the following options for configuring IP addresses:

- Configuration via V.24 connection
- Configuration using the HiDiscovery protocol
- Configuration via BOOTP
- Configuration via DHCP
- Configuration via DHCP Option 82
- Configuration using AutoConfiguration Adapter

Further information on the basic settings of the device can be found in the "Basic Configuration" user manual on the CD ROM.

Default settings

- IP address: The device looks for the IP address using DHCP
- Password for management:
  Login: user; password: public (read only)
  Login: admin; password: private (read and write)
- V.24 data rate: 9,600 Baud
- Ring redundancy: disabled
- Ethernet ports: link status is not evaluated (signal contact)
- Optical 100 Mbit/s ports: 100 Mbit/s, full duplex
  All other ports: autonegotiation
- Ring Manager disabled (DIP switch RM and stand-by: ON)
- Stand-by coupling disabled (DIP switch RM and stand-by: ON)
  Port 4 = control port, port 3 = coupling port for red. Ring coupling
- Rapid Spanning Tree enabled

USB interface

The USB socket has an interface for the local connection of an AutoConfiguration Adapter ACA 21-USB. It is used for saving/loading the configuration data and diagnostic information, and for loading the software.

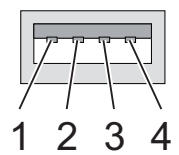
Figure	Pin	Function
	1	VCC (VBus)
	2	- Data
	3	+ Data
	4	Ground (GND)

Table 14: Pin assignment of the USB interface

V.24 interface (external management)

The V.24 interface is an RJ11 socket.
At the V.24 connection, a serial interface is provided for the local connection of an external management station (VT100 terminal or PC with corresponding terminal emulation) or an AutoConfiguration Adapter ACA 11. This enables you to set up a connection to the Command Line Interface (CLI) and to the system monitor.

VT 100 terminal settings	
Speed	9,600 Baud
Data	8 bit
Stopbit	1 bit
Handshake	off
Parity	none

The socket housing is electrically connected to the front panel of the device.
The V.24 interface is not electrically isolated from the supply voltage.

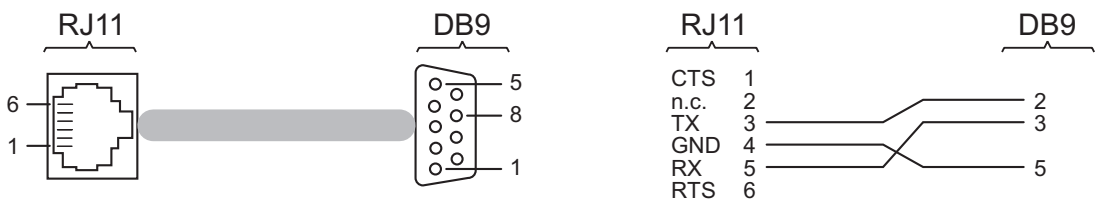


Figure 30: Pin assignment of the V.24 interface and the DB9 connector

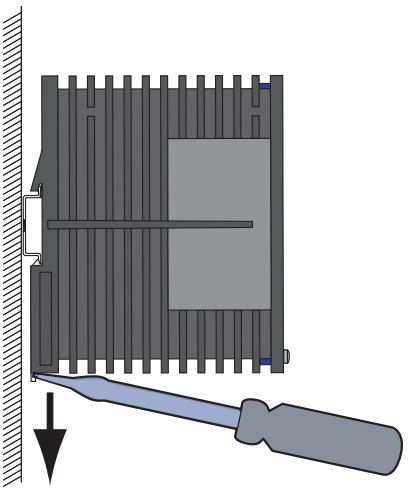
Note: You will find the order number for the terminal cable, which is ordered separately, in the Technical Data chapter (see page 60).

You will find a description of the V.24 interface in the “Basic Configuration User Manual” on the CD-ROM.

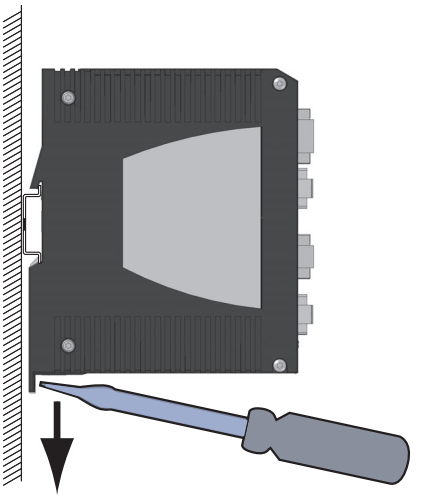
2.4 Disassembly

Removing the device from the DIN rail

☐ To take the device off the DIN rail, insert a screwdriver horizontally under the housing into the locking slide, pull it (without tipping the screwdriver) downwards and lift the device upwards.



RS20/RS30/RS40



RS22/RS32

Removing the device from the wall mounting plate

☐ To remove the device from the rail of the wall plate, press the device downwards and pull it from the rail below.

Disassembling the SFP modules

☐ Pull the module out of the socket by means of the opened lock.

☐ Close the module with the protective cap.

3 Technical data

General technical data

Dimensions W x H x D	RS20-0400...	47 mm x 131 mm x 111 mm
	RS20-08..., RS20-09..., RS30-0802	74 mm x 131 mm x 111 mm
	RS20-16..., RS20-17..., RS30-1602	110 mm x 131 mm x 111 mm
	RS20-24..., RS20-25..., RS30-2402	110 mm x 131 mm x 111 mm
	RS40-0009CCCCS...	74 mm x 131 mm x 111 mm
	RS40-0009CCCCE..., RS40-0009CCCCT...	110 mm x 131 mm x 111 mm
	RS22-08..., RS22-09..., RS32-0802	90 mm x 137 mm x 115 mm
	RS22-16..., RS22-17..., RS32-1602	120 mm x 137 mm x 115 mm
	RS22-24..., RS22-25..., RS32-2402	120 mm x 137 mm x 115 mm
	RPS 90/48V LV PoE power unit	60 mm x 137 mm x 115 mm
	RPS 90/48V HV PoE power unit	60 mm x 137 mm x 115 mm
Weight	RS20-0400...	400 g
	RS20-08..., RS20-09..., RS30-0802	410 g
	RS20-16..., RS20-17..., RS30-1602	600 g
	RS20-24..., RS20-25..., RS30-2402	650 g
	RS40-0009CCCCS...	530 g
	RS40-0009CCCCE..., RS40-0009CCCCT...	600 g
	RS22-08..., RS22-09..., RS32-0802	820 g
	RS22-16..., RS22-17..., RS32-1602	1150 g
	RS22-24..., RS22-25..., RS32-2402	1200 g
	RPS 90/48V LV PoE power unit	770 g
	RPS 90/48V HV PoE power unit	740 g
Power supply	Operating voltage RS20-..., RS30-..., RS40-...	
	Rated voltage range DC	12 to 48 V DC
	Max. voltage range DC	min. 9.6 to max. 60 V DC
	Rated voltage range AC	24 V AC
	Max. voltage range AC	min. 18 to max. 30 V AC Safety extra-low voltage (SELV), redundant inputs disconnected. Relevant for North America: NEC Class 2 power source max. 5A.
	Operating voltage RS22-..., RS32-...	48 V (47 V DC to 52 V DC) Safety extra-low voltage (SELV), redundant inputs disconnected. Relevant for North America: NEC Class 2 power source max. 5A.

PoE power unit RPS90/48V HV	Nominal voltage AC	110 - 230 V, 50 - 60 Hz
	Voltage range AC	90 - 265 V, 47 - 63 Hz (incl. max. tolerances)
	Power consumption at 110 V AC Power consumption at 230 V AC	1.00 A 0.50 A
	Nominal voltage DC	60 - 250 V
	Voltage range DC	48 - 320 V (incl. max. tolerances)
	Current consumption at 60 V DC Current consumption at 250 V DC	1.70 A 0.39 A
	Connection type	3-pin terminal block
	Output voltage	48 - 54 V DC (variable, default value: 48 V DC)
	Power output	At up to +60 °C: 90 W At +60 °C to +70 °C: 60 W
	Power failure bypass	> 10 ms
PoE power unit RPS90/48V LV	Nominal voltage DC	24 - 48 V
	Voltage range DC	18 - 60 V (incl. max. tolerances)
	Current consumption at 24 V DC Current consumption at 48 V DC	4.20 A 2.10 A
	Connection type	2-pin terminal block
	Output voltage	48 - 54 V DC (variable, default value: 48 V DC)
	Power output	At up to +60 °C: 90 W At +60 °C to +70 °C: 60 W
	Power failure bypass	> 10 ms
Overload current protection at input		Non-replaceable fuse
Insulation voltage between operating voltage connections and housing		800 V DC Protective elements limit the insulation voltage to 90 V DC (1mA)
“FAULT” signal contact	Switching current	max. 1 A, SELV
	Switching voltage	max. 60 V DC or max. 30 V AC, SELV
Environment	Storage temperature (ambient air)	Standard: -40 °C to +70 °C Extended: -40 °C to +85 °C
	Humidity	10% to 95% (non-condensing)
	Air pressure	Up to 2000 m (795 hPa), higher altitudes on request

Operating temperature	RS20/RS30/RS40	Standard: 0 °C to +60 °C Extended: -40 °C to +70 °C
	RS22-..., RS32-...	Extended: -40 °C to +50 °C
	RS40-...B... (ATEX) Standard (S)	Temperature Code T4: 0 °C to +60 °C
	RS40-...B... (ATEX) Extended (E and T)	Temperature Code T3: -40 °C to +70 °C Temperature Code T4: -40 °C to +60 °C
	RPS90/48V HV	-40 °C to +70 °C
	RPS90/48V LV	-40 °C to +70 °C Cold start at temperatures above -30 °C at an input voltage >= 21.6 V DC
Pollution degree		2
Protection classes	Laser protection	Class 1 according to EN 60825-1 (2001)
	Protection class	IP 20

EMC and immunity

EMC interference immunity		**A** [a)]	**B** [a)]	**H** [a)]
IEC/EN 61000-4-2	Electrostatic discharge			
	Contact discharge	4 kV	8 kV	8 kV
	Air discharge	8 kV	15 kV	15 kV
IEC/EN 61000-4-3	Electromagnetic field			
	80 - 3,000 MHz	10 V/m	20 V/m	20 V/m
IEC/EN 61000-4-4	Fast transients (burst)			
	Power line	2 kV	4 kV	4 kV
	Data line	1 kV	4 kV	4 kV
IEC/EN 61000-4-5	Voltage surges			
	Power line, line / line	0.5 kV	1 kV	1 kV
	Power line, line / earth	1 kV	2 kV	2 kV
	Data line	1 kV	4 kV	4 kV
IEC/EN 61000-4-6	Line-conducted interference voltages			
	10 kHz - 150 kHz	3 V	3 V	3 V
	150 kHz - 80 MHz	10 V	10 V	10 V
EN 61000-4-9	Impulse-shaped magnetic fields	—	300 A/m	300 A/m
EMC emitted interference		**A** [a)]	**B** [a)]	**H** [a)]
EN 55022	Class A	Yes	Yes	Yes
FCC 47 CFR Part 15	Class A	Yes	Yes	Yes
German Lloyd	Classification + Construction Guidelines VI-7-3 Part 1 Ed.2001	—	Yes	Yes
Stability		**A**[a]	**B** [a)]	**H** [a)]
Vibration	IEC 60068-2-6 Test FC test level according to IEC 61131-2	Yes	Yes	Yes
	Germanischer Lloyd Guidelines for the Performance of Type Tests Part 1	—	Yes	Yes

Stability		A[a]	B [a)]	H [a)]
	IEC 870-2-2 table 3 normal installation according to EN 61850-3	—	Yes	Yes
Shock	IEC 60068-2-27 Test Ea test level according to IEC 61131-2	Yes	Yes	Yes
	IEC 870-2-2 table 3 normal installation according to EN 61850-3	—	Yes	Yes

a. Product code A: Certification = CE, UL
Product code B: Certification = CE, UL, GL, railway (along track), sub station, ATEX
Product code H: Certification = CE, UL, GL, railway (along track), sub station
(s. page 16 ”Combination options for RS20/30“ and page 19 ”Combination options for RS40“)

Network range

TP port	
Length of a twisted pair segment	max. 100 m / 328 ft (cat5e cable with 1000BASE-T)

Table 15: TP port 10BASE-T / 100BASE-TX / 1000BASE-T

Product code		Wave length	Fiber	System attenuation	Expansion	Fiber data
-M2, -MM	MM	1300 nm	50/125 µm	0-8 dB	0-5 km	1.0 dB/km, 800 MHz*km
-M2, -MM	MM	1300 nm	62.5/125 µm	0-11 dB	0-4 km	1.0 dB/km, 500 MHz*km
-S2, -VV	SM	1300 nm	9/125 µm	0-16 dB	0-30 km	0.4 dB/km; 3.5 ps/(nm*km)
-E2, EE	SM+	1300 nm	9/125 µm	7-29 dB	20-65 km	0.4 dB/km; 3.5 ps/(nm*km)
-L2, -LL	LH	1550 nm	9/125 µm	7-29 dB	24-86 km	0.3 dB/km; 19 ps/(nm*km)
-G2, -GG	LH+	1550 nm	9/125 µm	14-47 dB	67-176 km	0.25 dB/km; 19 ps/(nm*km)

Table 16: F/O port 100BASE-FX

Product code M-FAST SFP-...		Wave length	Fiber	System attenuation	Expansion	Fiber data
-MM/LC...	MM	1310 nm	50/125 µm	0-8 dB	0-5 km	1.0 dB/km, 800 MHz*km
-MM/LC...	MM	1310 nm	62.5/125 µm	0-11 dB	0-4 km	1.0 dB/km, 500 MHz*km
-SM/LC...	SM	1310 nm	9/125 µm	0-13 dB	0-25 km	0.4 dB/km; 3.5 ps/(nm*km)
-SM+/ LC...	SM	1310 nm	9/125 µm	10-29 dB	25-65 km	0.4 dB/km; 3.5 ps/(nm*km)
-LH/LC	SM	1550 nm	9/125 µm	10-29 dB	40-104 km	0.25 dB/km; 19 ps/(nm*km)

Table 17: Fiber port 100BASE-FX (SFP fiber optic Fast ETHERNET Transceiver)

Product code M-SFP-...		Wave length	Fiber	System attenuation	Expansion	Fiber data
-SX/LC...	MM	850 nm	50/125 µm	0-7.5 dB	0-550 m	3.0 dB/km, 400 MHz*km
-SX/LC...	MM	850 nm	62.5/125 µm	0-7.5 dB	0-275 m	3.2 dB/km, 200 MHz*km
-MX/LC...	MM	1310 nm	50/125 µm	0-8 dB	2 km [a]	1.0 dB/km, 500 MHz*km
-MX/LC	MM	1310 nm	62.5/125 µm	0-8 dB	1 km	1.0 dB/km, 500 MHz*km
-LX/LC...	MM	1310 nm[b]	50/125 µm	0-11 dB	0-550 m	1.0 dB/km, 800 MHz*km
-LX/LC...	MM	1310 nm [b]	62.5/125 µm	0-11 dB	0-550 m	1.0 dB/km, 500 MHz*km
-LX/LC...	SM	1310 nm	9/125 µm	0-11 dB	0-20 km	0.4 dB/km; 3.5 ps/(nm*km)
-LX+/LC	SM	1310 nm	9/125 µm	5-20 dB	14-42 km	0.4 dB/km; 3.5 ps/(nm*km)
-LH/LC...	LH	1550 nm	9/125 µm	6-22 dB	24-72 km	0.25 dB/km; 19 ps/(nm*km)
-LH+/LC	LH	1550 nm	9/125 µm	15-30 dB	71-108 km	0.25 dB/km; 19 ps/(nm*km)
-LH+/LC	LH	1550 nm	9/125 µm	15-30 dB	71-128 km	0.21 dB/km (typical); 19 ps/(nm*km)

Table 18: Fiber port 1000BASE-FX (SFP fiber optic Gigabit ETHERNET Transceiver)

a. Distances up to 3 km reachable, 1000 MHz*km (1300 nm)
b. With F/O adapter compliant with IEEE 802.3-2002 clause 38 (single-mode fiber offset-launch mode conditioning patch cord)

MM = Multimode, SM = Singlemode, LH = Singlemode Longhaul

Power consumption/power output

Device name		Device model	Maximum power consumption	Power output
2 uplink ports:				
RS20-0400...		2xTX port	5.3 W	18.1 Btu (IT)/h
RS20-0400...		1xFX port, 1xTX port	6.5 W	22.2 Btu (IT)/h
RS20-0400...		2xFX port	7.7 W	26.3 Btu (IT)/h
RS20-0800...	RS22-0800...	2xTX port	5.3 W	18.1 Btu (IT)/h
RS20-0800...	RS22-0800...	1xFX port, 1xTX port	6.5 W	22.2 Btu (IT)/h
RS20-0800...	RS22-0800...	2xFX port	7.7 W	26.3 Btu (IT)/h
RS20-1600...	RS22-1600...	2xTX port	9.4 W	32.1 Btu (IT)/h
RS20-1600...	RS22-1600...	1xFX port, 1xTX port	10.6 W	36.2 Btu (IT)/h
RS20-1600...	RS22-1600...	2xFX port	11.8 W	40.3 Btu (IT)/h
RS20-2400-...	RS22-2400-...	2xTX port	12.1 W	41.3 Btu (IT)/h
RS20-2400-...	RS22-2400-...	1xFX port, 1xTX port	13.3 W	45.4 Btu (IT)/h
RS20-2400-...	RS22-2400-...	2xFX port	14.5 W	52.9 Btu (IT)/h
RS30-0802-...	RS32-0802-...	2xTX port	8.9 W	30.4 Btu (IT)/h
RS30-0802-...	RS32-0802-...	1xFX port, 1xTX port	8.6 W	29.4 Btu (IT)/h
RS30-0802-...	RS32-0802-...	2xFX port	8.3 W	28.4 Btu (IT)/h
RS30-1602-...	RS32-1602-...	2xTX port	13.0 W	44.4 Btu (IT)/h
RS30-1602-...	RS32-1602-...	1xFX port, 1xTX port	12.7 W	43.4 Btu (IT)/h
RS30-1602-...	RS32-1602-...	2xFX port	12.4 W	42.4 Btu (IT)/h
RS30-2402-...	RS32-2402-...	2xTX port	15.7 W	53.6 Btu (IT)/h
RS30-2402-...	RS32-2402-...	1xFX port, 1xTX port	15.4 W	52.6 Btu (IT)/h
RS30-2402-...	RS32-2402-...	2xFX port	15.1 W	51.6 Btu (IT)/h
3 uplink ports:				
RS20-0900-...	RS22-0900-...	3xFX port	9.6 W	32.8 Btu (IT)/h
RS20-1700-...	RS22-1700-...	3xFX port	13.7 W	46.7 Btu (IT)/h
RS20-2500-...	RS22-2500-...	3xFX port	16.4 W	56.0 Btu (IT)/h
4 uplink ports:				
RS30-0802-...	RS32-0802-...	4xFX port	12.7 W	43.3 Btu (IT)/h
RS30-1602-...	RS32-1602-...	4xFX port	16.8 W	57.3 Btu (IT)/h
RS30-2402-...	RS32-2402-...	4xFX port	19.5 W	66.5 Btu (IT)/h
RS40-...		4xFX port	20.0 W	68.2 Btu (IT)/h

Table 19: Power consumption/power output RS20/RS30/RS40 and RS22/RS32 without PDs (powered devices)

Device name	Device model	Maximum power consumption	Power output
2 uplink ports:			
RS22-0800...	2xTX port	70.9 W	31.8 Btu (IT)/h
RS22-0800...	1xFX port, 1xTX port	72.1 W	35.9 Btu (IT)/h
RS22-0800...	2xFX port	73.3 W	40.0 Btu (IT)/h
RS22-1600...	2xTX port	75.0 W	45.8 Btu (IT)/h
RS22-1600...	1xFX port, 1xTX port	76.2 W	49.9 Btu (IT)/h
RS22-1600...	2xFX port	77.4 W	54.0 Btu (IT)/h
RS22-2400-...	2xTX port	77.7 W	55.0 Btu (IT)/h
RS22-2400-...	1xFX port, 1xTX port	78.9 W	59.1 Btu (IT)/h
RS22-2400-...	2xFX port	80.1 W	66.6 Btu (IT)/h
RS32-0802-...	2xTX port	74.5 W	44.1 Btu (IT)/h
RS32-0802-...	1xFX port, 1xTX port	74.2 W	43.1 Btu (IT)/h
RS32-0802-...	2xFX port	73.9 W	42.1 Btu (IT)/h
RS32-1602-...	2xTX port	78.6 W	58.1 Btu (IT)/h
RS32-1602-...	1xFX port, 1xTX port	78.3 W	57.1 Btu (IT)/h
RS32-1602-...	2xFX port	78.0 W	56.1 Btu (IT)/h
RS32-2402-...	2xTX port	81.3 W	67.3 Btu (IT)/h
RS32-2402-...	1xFX port, 1xTX port	81.0 W	66.3 Btu (IT)/h
RS32-2402-...	2xFX port	80.7 W	65.3 Btu (IT)/h
3 uplink ports:			
RS22-0900-...	3xFX port	75.2 W	46.5 Btu (IT)/h
RS22-1700-...	3xFX port	79.3 W	60.4 Btu (IT)/h
RS22-2500-...	3xFX port	82.0 W	69.7 Btu (IT)/h
4 uplink ports:			
RS32-0802-...	4xFX port	78.3 W	57.0 Btu (IT)/h
RS32-1602-...	4xFX port	82.4 W	71.0 Btu (IT)/h
RS32-2402-...	4xFX port	85.1 W	80.2 Btu (IT)/h

Table 20: Power consumption/power output RS22/RS32 with 4 x Class0 PD (powered device)

Scope of delivery

Device	Scope of delivery
RS20-..., RS30-..., RS40-..., RS22-... or RS32-...	Device
	Terminal block for supply voltage and signal contact
	Installation user manual and CD-ROM
RS22-16..., RS22-17..., RS22-24..., RS22-25...	Additionally: ferrite with key

Order numbers/product description

See table on page 16 ”Combination options for RS20/30“ and table on page 19 ”Combination options for RS40“.

Accessories

Name	Operating temperature (chassis)	Order number
6-pin terminal block (50 pcs.)		943 845-006
AutoConfiguration Adapter ACA 11		943 751-001
AutoConfiguration Adapter ACA 21-USB		943 271-001
HiVision Network Management software		943 471-100
OPC Server software HiOPC		943 055-001
RPS 90/48V HV (high-voltage) PoE power unit		943 979-001
RPS 90/48V HV (high-voltage) PoE power unit with conformal coating		943 979-101
RPS 90/48V LV (low-voltage) PoE power unit		943 980-001
RPS 90/48V LV (low-voltage) PoE power unit with conformal coating		943 980-101
Pocket Guide		280 710-851
Rail Power Supply RPS 30		943 662-003
Rail Power Supply RPS 80 EEC		943 662-080
Rail Power Supply RPS 120 EEC		943 662-120
Terminal cable		943 301-001
Wall mounting plate for mounting the RS22/ RS32 on the wall		
Wall mounting plate, width 120 mm		943 971-001
Wall mounting plate, width 90 mm		943 971-002
Wall mounting plate, width 60 mm		943 971-003
Gigabit ETHERNET SFP Transceiver		
M-SFP-SX/LC	0 °C to +60 °C	943 014-001
M - SFP - SX / LC EEC	-40 °C to +70 °C	943 896-001
M - SFP - MX / LC	0 °C to +60 °C	942 035-001
M-SFP-LX/LC	0 °C to +60 °C	943 015-001
M - SFP - LX / LC EEC	-40 °C to +70 °C	943 897-001
M - SFP - LX+ / LC	0 °C to +60 °C	942 023-001
M - SFP - LX+/ LC EEC	-40 °C to +70 °C	942 024-001
M-SFP-LH/LC	0 °C to +60 °C	943 042-001
M - SFP - LH / LC EEC	-40 °C to +70 °C	943 898-001
M-SFP-LH+/LC	0 °C to +60 °C	943 049-001
Fast ETHERNET SFP Transceiver		
M-FAST SFP-MM/LC	0 °C to +60 °C	943 865-001
M-FAST SFP-MM/LC EEC	-40 °C to +70 °C	943 945-001
M-FAST SFP-SM/LC	0 °C to +60 °C	943 866-001
M-FAST SFP-SM/LC EEC	-40 °C to +70 °C	943 946-001
M-FAST SFP-SM+/LC	0 °C to +60 °C	943 867-001
M-FAST SFP-SM+/LC EEC	-40 °C to +70 °C	943 947-001
M-FAST SFP-LH/LC	0 °C to +60 °C	943 868-001
M-FAST SFP-LH/LC EEC	-40 °C to +70 °C	943 948-001
Bidirectional Gigabit ETHERNET SFP Transceiver		
M-SFP-BIDI Type A LX/LC EEC	-40 °C to +85 °C	943 974-001

Name	Operating temperature (chassis)	Order number
M-SFP-BIDI Type B LX/LC EEC	-40 °C to +70 °C	943 974-002
M-SFP-BIDI Type A LH/LC EEC	-40 °C to +70 °C	943 975-001
M-SFP-BIDI Type B LH/LC EEC	-40 °C to +70 °C	943 975-002
M-SFP-BIDI Bundle LX/LC EEC (Type A + B)	-40 °C to +70 °C	943 974-101
M-SFP-BIDI Bundle LH/LC EEC (Type A + B)	-40 °C to +70 °C	943 975-101

Underlying norms and standards

Name	
cUL 508:1998	Safety for Industrial Control Equipment
EN 50121-4:2006	Railway applications - EMC - emitted interference and interference immunity for signal and telecommunication systems
EN 55022:2006 + A1:2007	IT equipment – radio interference characteristics
EN 60079-15	Electrical equipment for explosive gas atmospheres – part 15: Construction, testing and marking of protection type "n" electrical apparatus.
EN 61000-6-2:2005	Generic norm – immunity in industrial environments
EN 61131-2:2007	Programmable logic controllers
FCC 47 CFR Part 15:2009	Code of Federal Regulations
Germanischer Lloyd	Ship Applications - Classification and Construction Guidelines VI-7-3 Part 1 Ed.2003
IEC/EN 60950-1:2006	Safety for the installation of IT equipment
IEC/EN 61850-3	Communications networks and systems in stations
IEEE 802.1 D	Switching, GARP, GMRP, Spanning Tree
IEEE 802.1 D-1998	Media access control (MAC) bridges (includes IEEE 802.1p Priority and Dynamic Multicast Filtering, GARP, GMRP)
IEEE 802.1 Q	Tagging
IEEE 802.1 Q-1998	Virtual Bridged Local Area Networks (VLAN Tagging, GVRP)
IEEE 802.1 w.2001	Rapid Reconfiguration
IEEE 802.3-2002	Ethernet
IEEE 1613	Standard Environment and Testing Requirements for Communication Networking Devices in Electric Power Substations
ISA 12.12.01 (cUL 1604), CSA C22.2 No. 213	Electrical Equipment for Use in Class I and Class II, Div.2 and Class III Hazardous (Classified) Locations
KR	Korean Register of Shipping

Table 21: List of norms and standards

The device has a certification based on a specific standard only if the certification indicator appears on the housing.
However, with the exception of Germanischer Lloyd, ship certifications as well as RINA certifications are only included in the product information under www.beldensolutions.com.
Use shielded twisted pair cables to fulfill the more stringent EMC requirements for the particular certifications.

A Further Support

Technical Questions and Training Courses

In the event of technical queries, please contact your local Hirschmann distributor or Hirschmann office.
You can find the addresses of our distributors on the Internet:
www.beldensolutions.com.

Our support line is also at your disposal:

- Tel. +49 1805 14-1538
- Fax +49 7127 14-1551

Answers to Frequently Asked Questions can be found on the Hirschmann internet site (www.beldensolutions.com) at the end of the product sites in the FAQ category.
The current training courses to technology and products can be found under http://www.hicomcenter.com.

Hirschmann Competence Center

In the long term, excellent products alone do not guarantee a successful customer relationship. Only comprehensive service makes a difference worldwide. In the current global competition scenario, the Hirschmann Competence Center is ahead of its competitors on three counts with its complete range of innovative services:

- Consulting incorporates comprehensive technical advice, from system evaluation through network planning to project planing.
- Training offers you an introduction to the basics, product briefing and user training with certification.
- Support ranges from the first installation through the standby service to maintenance concepts.

With the Hirschmann Competence Center, you have decided against making any compromises. Our client-customized package leaves you free to choose the service components you want to use.
Internet:
http://www.hicomcenter.com.

HIRSCHMANN

A BELDEN BRAND